Copy 6 S/S 27 Sept 94

FM 34-1

JULY 1987

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited

Pentagon Library (ANR-PL)
ATTN: Military Documents Section
Room 1A518, Pentagon
Washington, DC 20310-6050

Copy b

FIELD MANUAL
NO. 34-1

*FM 34-1

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 2 July 1987

INTELLIGENCE AND ELECTRONIC WARFARE OPERATIONS

Table of Contents

		Page
Preface		**iv**
Chapter 1	**— The Mission**	**1-1**
	Situation and Target Development	**1-1**
	Electronic Warfare	**1-3**
	Counterintelligence	**1-4**
Chapter 2	**— The Intelligence and Electronic Warfare System**	**2-1**
	Functional Structure	**2-1**
	Coordination Structure	**2-4**
	System Elements	**2-20**
	Echelon Architecture	**2-21**
Chapter 3	**— Situation and Target Development**	**3-1**
	Intelligence Preparation of the Battlefield	**3-3**
	Collection Management	**3-20**
	Processing	**3-38**
	Dissemination	**3-60**
Chapter 4	**— Counterintelligence**	**4-1**
	Support to Operations Security	**4-1**
	Support to Rear Operations	**4-10**
	Support to Deception	**4-13**
	Support to Command, Control, and Communications Countermeasures	**4-15**
Chapter 5	**— Electronic Warfare**	**5-1**
	Electronic Warfare Section	**5-1**
	Electronic Countermeasures	**5-2**
	Electronic Warfare Targets	**5-7**
	Electronic Warfare Principles	**5-9**

Distribution Restriction: Approved for public release; distribution is unlimited.

*This publication supersedes FM 34-1, 31 August 1984.

Pentagon Library (ANR-PL)
ATTN: Military Documents Section
Room 1A518, Pentagon
Washington, DC 20310-6050

Electronic Warfare Planning 5-10
Electronic Warfare Tasking 5-14
Electronic Warfare Assessment 5-14

Chapter 6 — Organization for Combat 6-0
Command and Support Relationships 6-0
Principles of Organization 6-1
Task Organization 6-1
Communications 6-4

Chapter 7 — Offensive Operations 7-0
IEW Principles 7-0
Support to Offensive 7-1
River Crossing 7-7

Chapter 8 — Defensive Operations 8-0
IEW Principles 8-0
Deep Operations 8-2
Covering Force 8-3
Support to the Main Battle 8-7

Chapter 9 — Retrograde Operations 9-0
IEW Principles 9-0
Delaying 9-1
Withdrawal 9-4
River Crossings 9-6

Chapter 10 — Defense and Breakout of Encircled Forces 10-0
Defense 10-0
Breakout 10-2

Chapter 11 — Rear Operations 11-1
Air-Land Battle Tenets 11-1
Objectives 11-2
Threat 11-2
Command and Control 11-6
Intelligence Mission 11-14
Intelligence and Electronic Warfare Support 11-17

Chapter 12 — Special Operations and Environments 12-0
Special Operations 12-0
Special Environments 12-7

Chapter 13 — Joint and Combined Operations 13-0
Joint Operations 13-0
Contingency Operations 13-6
Combined Operations 13-6

Chapter 14 — Logistics 14-1
Supply 14-1
Maintenance, Repair, and Recovery 14-7
MI Unit Maintenance 14-11
Replacement 14-11

Chapter 15 — **NBC Survival and Reconstitution** **15-0**
Effects **15-0**
Vulnerabilities **15-1**
Survival **15-2**
Reconstitution **15-4**

Appendix A - **The Analysis of the Battlefield Area** **A-1**
Appendix B - **The Intelligence Estimate** **B-1**
Appendix C - **The Intelligence Annex** **C-1**
Appendix D - **The Electronic Warfare Estimate** **D-1**
Appendix E - **The Electronic Warfare Annex** **E-1**
Appendix F - **Electronic Warfare Targeting Formats** **F-0**
Appendix G - **Dissemination Devices** **G-1**
Appendix H - **The Collection Plan** **H-1**
Appendix I - **Tactical Special Security Operations** **I-1**
Glossary **Glossary-0**
References **References-0**
Index **Index-1**

Preface

Intelligence and electronic warfare (IEW) is critical to the US Army's fundamental mission of winning air-land battles. During peacetime, the IEW system provides the intelligence and counterintelligence (CI) and defensive electronic warfare (EW) support essential to deterring war through vigilance and preparedness. During war, these mission areas and the addition of offensive EW, focus on supporting the winning of battles and campaigns.

This IEW keystone manual expands doctrine contained in FM 100-5, and establishes the doctrinal foundation for IEW operations. It delineates the IEW mission on the modern battlefield, the IEW role in maximizing the combat power of the combined arms team, the principles which govern tactical IEW operations, and the importance of sustaining IEW capabilities. The doctrine in this manual orients on principles and general procedures and is based on applicable Army of Excellence (AOE) tables of organization and equipment (TOE). More specific operational procedures are provided in doctrinal field manuals.

This manual is designed for use by commanders, staffs, and trainers at all echelons. It is the foundation for Army service school IEW instruction and serves as the basis for IEW doctrinal, training, and combat developments.

Provisions of this manual are subject to international standardization agreements (STANAGs) 2008, 2014, 2022, and 3377. STANAG 2014 (Edition Five) is implemented by Appendixes C and E to this field manual. When amendment, revision, or cancellation of this publication affects or violates the international agreements concerned, the preparing agency will take appropriate reconciliation action through international standardization channels.

The proponent of this publication is the United States Army Intelligence Center and School. Submit changes for improving this publication on DA Form 2028 (Recommended Changes to Publications and Blank Forms) and forward to Commander, US Army Intelligence Center and School, ATTN: ATSI-TD-PAL, Fort Huachuca, AZ 85613-7000.

CHAPTER 1

The Mission

Armies that maintain coherence and confidence and can concentrate superior combat power at decisive times and places are the winners of battles and campaigns. While there are no simple formulas for winning, there are certain key factors for success on the air-land battlefield. One key factor is the support provided to the combined arms team through IEW operations.

IEW operations, in both peace and war, support the winning of battles and campaigns—the focus of tactical doctrine described in FM 100-5. The mission of IEW operations is to provide the maneuver commander with three key forms of support: intelligence, EW, and CI.

History is full of examples of the vital role intelligence plays in combat operations. There have been many instances in which forces with superior intelligence have been victorious over much larger opposing armies. Commanders who have possessed detailed knowledge of the enemy, weather, and terrain and used that knowledge in their application of fire and maneuver have usually been the victors. General Washington's surprise attack on Trenton and the 1942 American victory at Midway, the turning point in the battle for the Pacific, are shining examples of the value of accurate intelligence. More recent history has demonstrated the advantages of using EW and CI. EW, especially its use in the 1973 Arab-Israeli war, and in 1982 in the Bekaa Valley, has proven itself a credible weapon for both offensive and defensive purposes. The need for CI and its value as a principal contributor to the security of the combat force were proven during Korea, Vietnam, and the intervening years of peace. These support functions will be of equal or greater value in the air-land battle of today. Successful execution of the IEW mission will be critical on the air-land battlefield.

The combined application of these forms of support, the IEW mission, translates into four major tasks: situation development, target development, EW, and CI.

SITUATION AND TARGET DEVELOPMENT

Situation development is the basic process by which intelligence is developed. Information is collected, then integrated into an all-source product to provide an estimate of the situation and a projection of enemy intentions in sufficient time to permit the commander to select the most effective friendly course of action. Situation development provides—

- Knowledge of the weather and terrain throughout the areas of operations and interest.
- Knowledge of the enemy to include enemy organization, equipment, and tactics—how the enemy fights; the strengths and weaknesses of enemy dispositions; the capabilities, limitations, and patterns of particular enemy units; the enemy's operational, technical, and human weaknesses and personalities; the enemy's intentions; and the enemy's probable reactions.

Weather and terrain have more impact on the battle than any other physical factor, including weapons, equipment, or supplies. The terrain on which battles are fought presents opportunities to both sides. Most battles have been won by the side that used terrain to protect itself and to reinforce fires to destroy the enemy. Commanders must understand the nature, uses, and reinforcement of terrain to be effective.

IEW operations assist commanders in selecting and understanding the battlefields on which they choose to fight. Intelligence preparation of the battlefield (IPB), a systematic approach to the analysis of enemy, weather, and terrain, is the principal tool used. It clearly portrays what enemy forces can and cannot do on the battlefield and the probability of the adoption of a specific course of action. It also is used to clearly show the effects of weather and terrain on

friendly forces and courses of action. IPB is begun long before the battle and is updated continually.

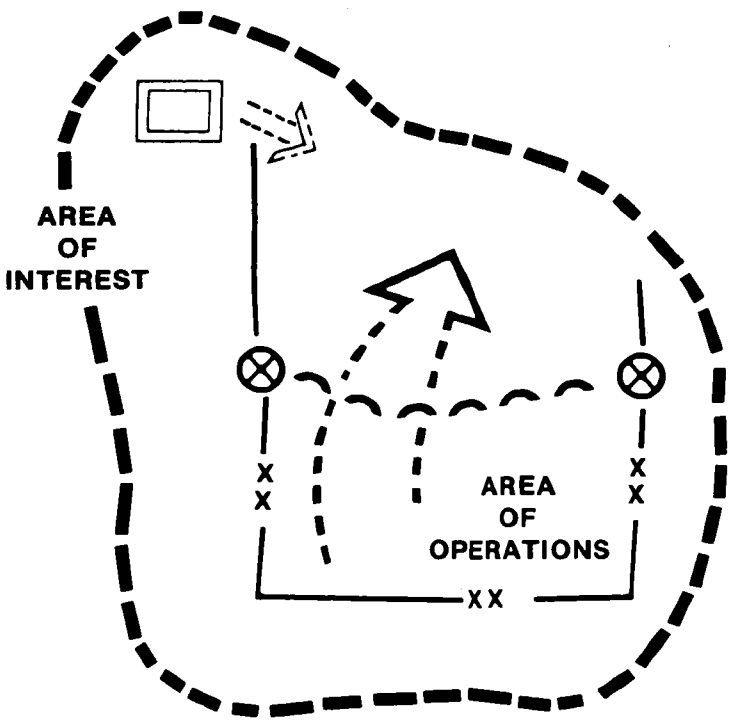
To succeed in battle, commanders must avoid enemy strengths and exploit weaknesses. They must surprise enemy forces, catching them at a disadvantage as often as possible. IPB provides the basis for the situation and target development tasks which make this possible. Situation development reduces battlefield uncertainty and provides the confidence to generate superior combat power.

Target development, based on situation development, is the process of providing direct combat information, targeting data, and correlated targeting information to commanders and fire support means. It provides the commander with timely and accurate locations of enemy weapons systems, units, and activities which may impact on current or projected operations. Targeting data must be sufficiently timely and accurate to support effective attack by fire, maneuver, or electronic means.

Situation and target development provide commanders with the intelligence they need to fight the air-land battle. Both are distinct tasks, yet they must be integrated totally to provide an accurate picture of the battlefield and to assist in successful accomplishment of the friendly commander's intent. Both tasks focus the areas of operations and interest.

The battlefield is comprised of the area of operations (AO), and the area of interest. Commanders and staffs view these areas in terms of width, depth, airspace, and time.

BATTLEFIELD AREAS



The AO is defined in JCS Pub. 1 as "that portion of an area of conflict necessary for military operations." The AO is a geographical area, assigned by a higher commander, for which a commander has responsiblity and in which he has authority to conduct military operations. Higher commanders consider the factors of mission, enemy, terrain, troops, and time available (METT-T) when assigning AOs.

The area of interest is defined in JCS Pub. 1 as "that of concern to the commander, including the area of operations, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces which could jeopardize the accomplishment of the mission." The area of interest overlaps those of adjacent and higher units, to include areas to the rear of the AO.

AOs and area of interest help to focus the information requirements of commanders from battalion to echelons above corps (EAC). Specific information requirements are dependent on the mission and the tactical situation. Usually, in conventional battles, information requirements are based on the one-up-and-two-down formula. Commanders require detailed information about enemy forces at their equivalent levels of command as well as at one level above and two levels below their own. For example, brigade commanders need information about enemy regiments (equivalent level), enemy divisions (one up), and enemy battalions and companies (two down). Generally, the enemy forces of concern to each commander are found within the command's AO and area of interest.

ELECTRONIC WARFARE

EW exploits, disrupts, and deceives the enemy command and control (C^2) system while protecting friendly use of communications and noncommunications systems. It is a significant force multiplier when integrated and employed with fire and maneuver.

EW represents a significant contributor to command, control, and communications countermeasures (C^3CM). C^3CM is the integrated use of operations security (OPSEC), military deception, jamming, and physical destruction to disrupt enemy C^2. C^3CM protects friendly command, control, and communications (C^3); influences, degrades, or destroys enemy C^3 capabilities; and denies the enemy information of intelligence value.

PROTECT COMMAND, CONTROL, AND COMMUNICATIONS

Electronic counter-countermeasures (ECCM), or defensive EW, are the responsibility of all soldiers who use or who supervise the use of communications-electronics (C-E) equipment. ECCM are passive in nature and are used to protect friendly C^3 systems against enemy radioelectronic combat (REC) activities. Passive ECCM include both anti-intercept and locate (for example, emission control, terrain masking, and avoidance) procedures and antijam or kill (for example, C-E equipment design) features. ECCM also include the immediate identification and reporting of meaconing, intrusion, jamming, and interference (MIJI) on a friendly C^3 facility.

Electronic warfare support measures (ESM) can provide commanders the capability to intercept, identify, and locate enemy emitters. They represent a source of information required for jamming, deception, ECCM, targeting, and other tactical employment of combat forces. ESM support the destruction and jamming of enemy C^3 systems through acquisition and reporting of targeting data. ESM also support the commander's efforts to counter enemy OPSEC and deception.

In extreme situations, electronic countermeasures (ECM) can be used to protect friendly C^3. Jamming systems may be used as high-powered radios to transmit a key message through enemy jamming. Additionally, jammers may protect friendly communications by using directional antennas to jam known enemy signals intelligence (SIGINT) systems on the same frequency as key friendly communications to screen and prevent enemy intercept. This option takes multiple jammers to cover the

deployed enemy collectors, and can place our jammers at great risk. Expandable jammers (EXJAMs) may also be used to screen friendly communications if their emplacement near enemy SIGINT sites is feasible.

COUNTER-COMMAND, CONTROL, AND COMMUNICATIONS

The offensive components of EW, passive ESM and active ECM, provide commanders—

- ☐ Intelligence to plan, direct, coordinate, support, and conduct their deep and close operations.
- ☐ Combat information and targeting data to maneuver their forces and target their weapons systems.
- ☐ ECM nonlethal attack capability to systematically disrupt the C^3 systems of enemy first- and second-echelon units.

CRITICAL TASKS

Command and control warfare in air-land combat operations is complex when viewed as a maze of intangible electronic signals criss-crossing above and over the battlefield. Command and control warfare, however, can be reduced to the most simple terms of reference and understanding. It is composed of both tangibles and intangibles. The tangibles are the C^3 "nodes" which present visual signatures for commanders to see and shoot. The intangibles are the "information links" between the nodes which can be intercepted, identified, and jammed. There are also nodes which can be intercepted, identified, and jammed. There are also nodes and links which must be seen and monitored, but neither shot nor jammed. Put simply, we jam and kill the fighters and sustainers, and collect information from the planners and coordinators.

COUNTERINTELLIGENCE

IEW operations must include specific actions which support the protection of the force. Through CI, IEW operations support actions which—

- ☐ Counter the hostile intelligence threat.
- ☐ Safeguard the command from surprise.
- ☐ Deceive the enemy commander.
- ☐ Counter enemy sabotage, subversion, and terrorism.

The need for commanders to know the enemy is not restricted to friendly force commanders. Enemy commanders, to succeed against us, must employ all-source intelligence systems to collect information about our forces. Depriving enemy commanders of this information is important, even crucial to friendly force success on the battlefield. CI supports the OPSEC of the command to achieve this objective.

Safeguarding the command from surprise includes two elements of IEW support. The first is intelligence which enables the commander to know the enemy's activities and intentions. The second is CI support to OPSEC which helps to deprive the enemy commander of the intelligence he needs to create situations in which the friendly force can be taken by surprise.

Deception is supported by intelligence which is critical to establishing a credible deception scenario and in assessing the effectiveness of deception operations. Electronic deception is supported and, to a limited degree, executed by the IEW system.

IEW contributes significantly to the protection of the force by CI operations against sabotage, subversion, and terrorism. These operations prevent hostile actions which disrupt the sustainment of combat operations and undermine morale, cohesion, and discipline.

Each of the major tasks derived from the IEW mission is essential to success on the battlefield. How IEW operations fulfill the requirements of each task, IEW employment for specific operations, and the critical functions of sustaining operations is explained in general terms in the chapters which follow. The doctrine presented is based on, and requires an understanding of, the air-land battle doctrine of FM 100-5.

CHAPTER 2

The Intelligence and Electronic Warfare System

This chapter describes the IEW system. It begins with the design philosophy of the system, describes its functional structure, then shows how the functional resources are welded into an interlocking organization at each level of command to provide the intelligence, EW, and CI support so critical to the commander's success. This chapter describes the structure of the system in two ways: first, in terms of its functional structure, and second, in terms of its architecture by echelon.

FUNCTIONAL STRUCTURE

The IEW system design philosophy is embedded in a common IEW structure at each level of command. Each command has directors, coordinators, producers, and executors who perform critical IEW functions. The figure on page 2-2 illustrates the common IEW system structure.

Force commanders play a significant role in the design philosophy of the IEW system. Their requirements must be satisfied, their direction moves the system to respond, and their personal involvement keeps the system on track.

The coordinators are the G2 or S2 and G3 or S3. They have staff responsibility for coordinating the IEW effort. They respond to the commander as the functional experts in IEW, supervise and direct the operations of producers, and coordinate the efforts of the command's executors with support from higher, lower, and adjacent commands.

The G2 and S2 are the commanders' principal advisors for intelligence and CI operations and security policy. They plan and manage operations in each of these functional areas.

COMMON IEW STRUCTURE

DIRECTOR
FORCE COMMANDER

COORDINATORS

G2 AND S2
Intelligence
CI
Security

G3 AND S3
Operations
EW
OPSEC
Deception

PRODUCERS

Collection Management
Prepare collection plans
Manage collection activities

Analysis
IPB
Processing
Intelligence analysis
Enemy, weather, and terrain data bases

ESM
Technical data base support

OPSEC
OPSEC data base support
Vulnerability analysis
Countermeasure recommendation

Dissemination
Reports
Briefings
Estimates

EXECUTORS

COMMANDERS
MI
Cavalry
Artillery
Maneuver
Engineer
All Others

COMMAND
Direct and control organic assets to satisfy requirements

The director, coordinators, producers, and executors are common elements of the IEW structure at each command level.
The level of detail for each function varies by echelon.

The G2 and S2 coordinate the intelligence effort. They identify intelligence requirements based on the commanders' guidance and concept of the operation. They manage the collection effort, supervise all-source analysis, and ensure rapid dissemination of needed intelligence and combat information. They, through the division and corps tactical operations center (TOC) support elements, or brigade and battalion battlefield information coordination centers (BICC), task military intelligence (MI) organizations and other elements of the command with collection missions. The G2 and S2 request support and receive intelligence from higher echelons, adjacent units, other services, allies, and national sources. They integrate intelligence from all sources to meet the commanders' information and operational needs.

The G2 and S2 are responsible for information regarding the enemy, weather, and terrain. They use their expertise to reduce battlefield uncertainties, providing commanders with estimates and other critical intelligence in support of unit operations. They think like enemy commanders and view the battlefield from an enemy point of view. They direct the intelligence effort to view the patterns of enemy activity that serve as indicators, focusing on specific rather than general requirements. Their direction gives meaning to seemingly insignificant bits of information, and intelligence products of value to commanders are developed.

Generally, the responsibilities of the intelligence officer are similar at each level of command. The G2 or S2—

- ☐ Recommends intelligence requirements and priorities.
- ☐ Prepares plans, orders, and requests for intelligence, ESM, and CI.
- ☐ Supervises and coordinates the command's intelligence collection, ESM, and CI activities to support situation development and target development.
- ☐ Processes information from all available sources to produce intelligence.
- ☐ Assesses enemy intentions.
- ☐ Develops document and personnel security policy for the command.
- ☐ Supervises the command's special security officer (SSO).
- ☐ Supervises and directs the efforts of the engineer terrain team under his operational control (OPCON) and coordinates support from other teams.
- ☐ Exercises staff supervision of the staff weather officer (SWO).
- ☐ Supervises and coordinates predictions of fallout from enemy-employed nuclear weapons and chemical dispersion.
- ☐ Disseminates combat information and intelligence.
- ☐ Provides information and intelligence to other staff sections.
- ☐ Assesses enemy intelligence capabilities and procedures, their vulnerability to deception, and the effectiveness of friendly deception operations.
- ☐ Provides CI support to OPSEC.
- ☐ Prepares intelligence estimates and annexes.

FM 101-5 provides a detailed description of the responsibilities and functions of the G2 or S2.

The G3 and S3 have staff responsibility for planning and directing the OPSEC, deception, and EW operations of the command. They advise and assist other staff officers on the operations and training aspects which impact on their respective areas of responsibility. The G3 or S3—

- ☐ Plans and coordinates EW operations.
- ☐ Directs electronic countermeasures (ECM) actions needed to support planned and ongoing operations.
- ☐ Identifies, in coordination with the G2 or S2, as appropriate, ESM requirements to support EW.

- ☐ Coordinates with the C-E officer to establish ECCM to protect friendly C-E operations.
- ☐ Prepares the EW annex to operations plans (OPLAN) and orders.
- ☐ Identifies and recommends essential elements of friendly information (EEFI).
- ☐ Implements OPSEC measures to frustrate the enemy intelligence collection effort.
- ☐ Plans and coordinates deception operations to support the commanders' scheme of fire and maneuver.

FM 101-5 provides a detailed description of the responsibilities and functions of the G3 or S3.

The producers support the coordinators at each echelon. They perform collection management, information processing and dissemination, CI analysis, and EW management. At corps and division the producers consist of the TOC support elements. At lower echelons, they are the BICCs.

The BICCs assigned to various combat, combat support, and combat service support (CSS) units, give the unit S2 the capability to effectively manage his part of the IEW system. They are not a separate element, but an integral part of the S2 section. BICCs provide the detailed control and coordination of intelligence collection, production, and dissemination. They play a limited role in EW and OPSEC. BICCs not only expand the capabilities of the S2 sections, but free the S2 from routine tasks so he can better manage the overall intelligence effort.

The executors are the doers. They command the units which provide IEW support and direct and control them to satisfy assigned IEW missions. They deploy, maintain, train, and sustain their units to carry out assigned missions. Executors include the commanders of MI, cavalry, artillery, and maneuver units, and all other organizations capable of executing IEW operations. MI unit commanders are the command's primary IEW executors.

COORDINATION STRUCTURE

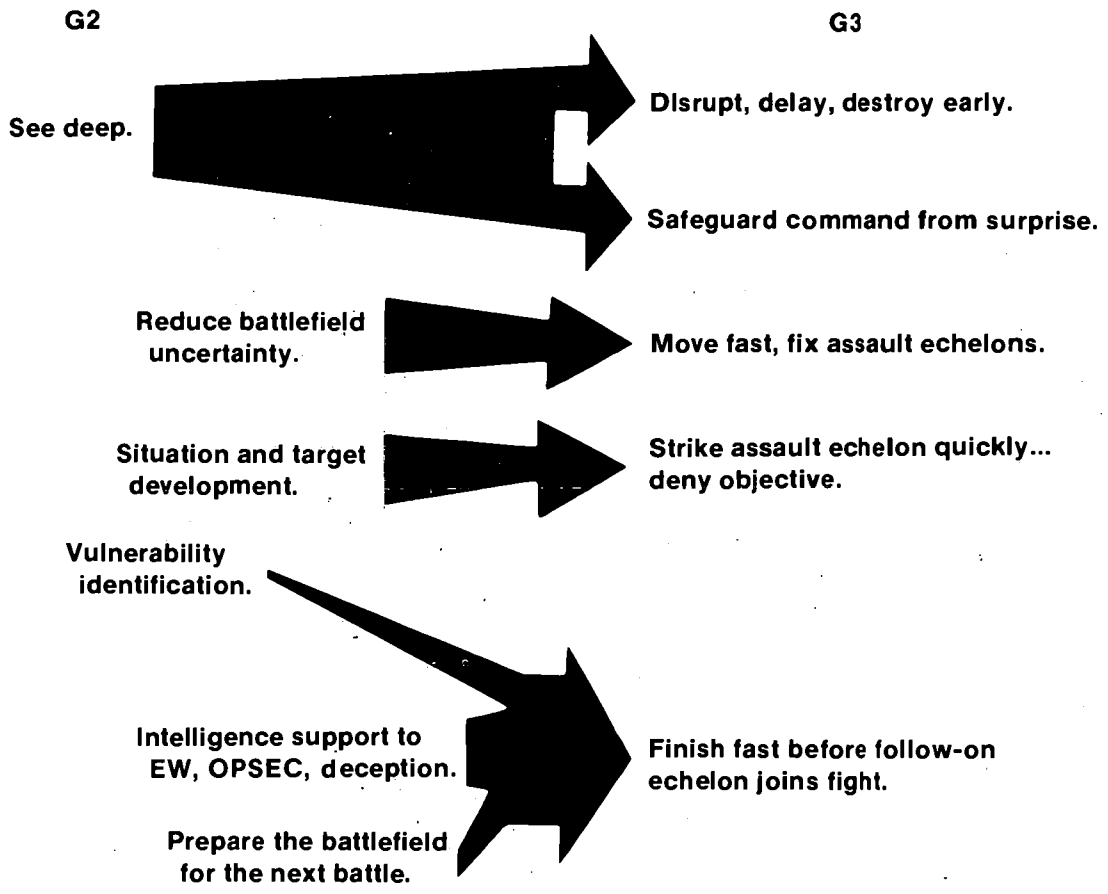
The key players in fusing IEW into the overall tactical concept are the intelligence and operations staffs. Their mission is to serve the commander and assist subordinate commanders.

The senior intelligence and operations officers must think like the commander in order to anticipate requirements. Both require a solid foundation in tactics to accomplish their missions. Their functions are reciprocal; both should be able to do the other's job. Their functions are complementary, requiring very close cooperation and coordination. Common perspectives enable them to communicate with precision. The senior intelligence and operations officers of the command, assist in the development and training of subordinate unit intelligence and operations staffs.

In coordinating the air-land battle, commanders demand complementing capabilities from their G2 and G3 as shown in the following illustration.

The G2, G3, and the MI commander comprise the IEW team. The staff officers plan, organize, direct, coordinate, and control while the MI commanders execute the directives. The IEW team is held together by the force commander who gives the team leadership, motivation, focused perspective, and direction.

DEVELOPING AIR-LAND BATTLE CAPABILITIES



The G2, as the command intelligence officer, provides overall management and supervision of intelligence operations. Based on the commander's requirements he develops intelligence collection missions and tasks subordinate elements, including organic and supporting MI units, to accomplish these missions. The G2 staff is augmented by the TOC support element, less the electronic warfare section (EWS) and OPSEC staff element. The G3 orchestrates EW and OPSEC operations. He develops EW and OPSEC missions based on requirements and tasks subordinate elements to carry them out. The G3 is augmented by the EWS and OPSEC staff element. MI unit commanders manage MI assets to accomplish assigned IEW missions. They exercise C^2 over all organic and attached MI elements and OPCON over supporting MI assets.

To fulfill the commander's requirements, the G2 and G3 must do the staff management necessary to translate capabilities into plans and orders for the combined arms team. Some of the specific staff functions associated with coordinating the battle are summarized in the following chart.

HOW G2s AND G3s ORCHESTRATE IEW OPERATIONS

PLANNING	ORGANIZING	DIRECTING	CONTROLLING	COORDINATING
Determine current and future needs. Study situation and limitations. Make reasonable assumptions. Perform detailed planning. Determine time and resource requirements to support plan. Ascertain requirement/resource balance. Adjust plan if necessary. Develop alternate plans. Establish policies/procedures to support plan. Use SOPs to speed communications and promote understanding.	Determine requirements to support mission. Establish work breakdown structure of tasks/subtasks. Establish organizational relationships. Select/assign resources to accomplish mission. Assign mission responsibilities. Emphasize essentiality, balance, cohesion, flexibility, and efficiency.	Determine extent of direction necessary. Issue timely instructions and mission tasking and ensure they are understood.	Determine extent, type, and method of control necessary to accomplish mission. Establish criteria for measuring results. Establish minimum variance from criteria that is acceptable. Take corrective action. Supervise execution. Monitor resource performance and sustainability.	Promote cooperation and mutual understanding. Cross-train supervisors and keep them informed. Encourage lateral and vertical communication throughout the organization. Synchronize requirements with external activities.

Each member of the IEW team has a full array of vital responsibilities. All of these responsibilities must be integrated, mutually supporting, and focused on the commander's concept for accomplishing the mission. Close and continuous coordination among all members of the team is essential. The following chart provides a graphic illustration of responsibilities and the coordination required to assure a fully integrated IEW operation.

IEW STAFF RESPONSIBILITIES

FUNCTIONS	STAFF RESPONSIBILITY	COORDINATION
INTELLIGENCE	G2	G3/FSE
IPB	G2	G3/FSE
Collection Management	G2	G3
Situation Development	G2	G3
Target Development	G2	G3/FSE
ELECTRONIC WARFARE	G3	G2/FSE/C-E OFFICER
ESM	G2	G3
ECM	G3	G2/FSE
ECCM	G3	G2/FSE/C-E OFFICER
OPSEC	G3	G2
CI Support	G2	G3
C^3CM	G3	G2/FSE
Intelligence Support	G2	G3/FSE/ALO
EW Support	G3	G2/FSE
OPSEC	G3	G2
Targeting	G3	G2/FSE/ALO

As depicted in the chart, the fire support element (FSE) is a key user of intelligence and plays an important role in EW planning. He is responsible for the integration of all lethal and non-lethal means of attack for the G3, which requires close coordination with the all-source production section (ASPS) and EWS in the division tactical operations center (DTOC).

No single level of command is capable of meeting all of its requirements with organic resources. Each is dependent on higher, lower, and adjacent commands to complete the intelligence picture of the battlefield, to meet EW requirements, or to support the security needs of the command. Therefore, commanders at each echelon must ensure that their resources are integrated into the overall IEW effort. For example, division depends on brigades and battalions for some information about first-echelon enemy battalions and regiments. It also depends on corps and EAC for information about second-echelon divisions. The interdependencies between echelons create the need for detailed interfaces. Such interfaces exist between the coordinators at successive echelons, between producers at division and higher levels, and between executors at division and higher levels. Additional interfaces are established laterally and, at EAC and corps, with other services, national agencies, and allied forces.

INTELLIGENCE

Battle success depends on the force commander's ability to see the battlefield. The enemy must be surprised and caught at a disadvantage as often as possible. Their

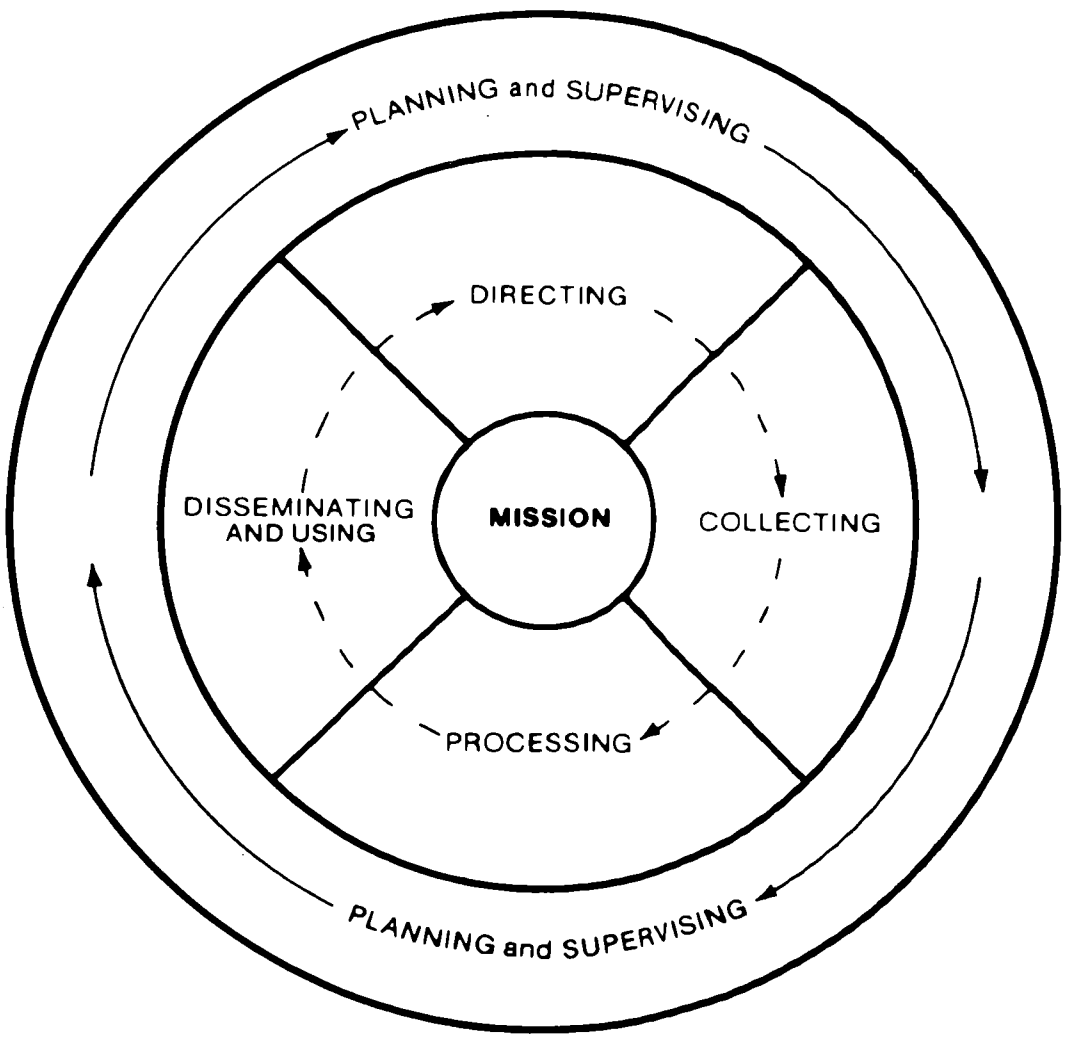
strengths must be avoided and their weaknesses exploited. To do this, commanders must know their battlefield area, the conditions in which they will fight, and the nature, capabilities, and activities of their enemy.

Intelligence: The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operations and which is immediately or potentially significant to military planning and operations.

Intelligence is the responsibility of all commanders. Every unit must be prepared to conduct intelligence operations with every means at its disposal, with or without specific orders.

Intelligence is developed through a process known as the intelligence cycle. The cycle, shown below, consists of four phases:

THE INTELLIGENCE CYCLE

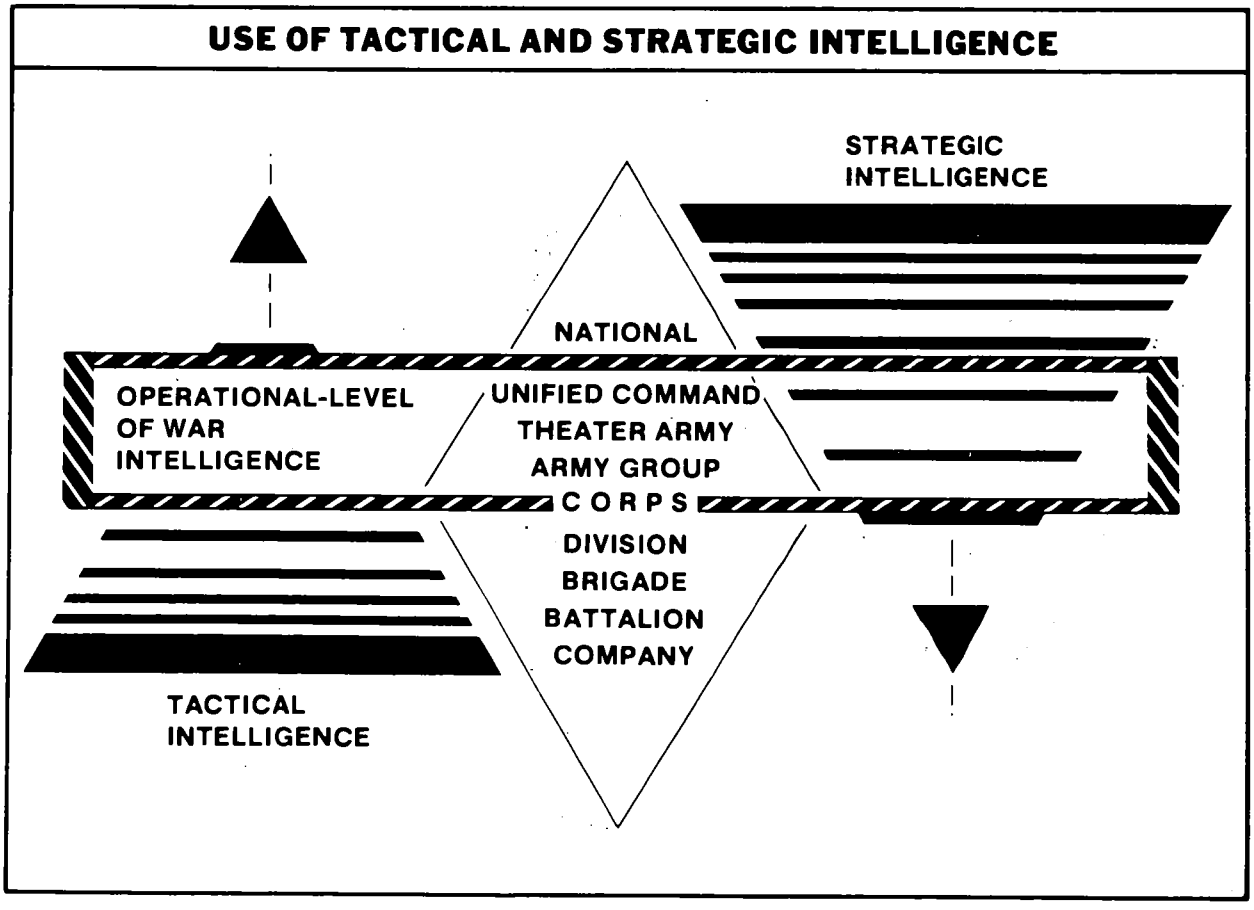


directing, collecting, processing, and disseminating. It is a continuous process, and even though each phase is conducted in sequence, all phases are conducted concurrently. While new information is being collected, the staff plans and redirects efforts to meet new demands, and previously collected information is processed and disseminated. All phases of the cycle focus on the commander's mission. (See the preceding illustration.)

Intelligence is categorized as strategic, operational level of war, and tactical. The focus and definition of each are tailored to the echelon and type of decision maker to be supported. (See illustration.) Strategic intelligence is defined as that intelligence required by national and allied decision makers for the formulation of national foreign and defense policy. The intelligence requirements of the National Command Authority (NCA) are global, reflecting the complexities of a continuously-evolving national interest and international context. The strategic intelligence community will collect, analyze, and disseminate intelligence which satisfies the constantly-changing requirements of national-level decision makers. As the imperatives of American foreign and defense policy change, so too does the focus of the strategic intelligence community.

The establishment of theater(s) of war or unified commands (assigned distinct geographical areas of operation) reflects the imperatives of American foreign and defense policy. While the intelligence requirements of the NCA are global, the intelligence requirements of the theater or unified commander in chief (CINC) will reflect the peculiar peacetime and wartime responsibilities assigned to that theater in the context of the Joint Strategic Capabilities Plan. The military strategy, force structure, and intelligence requirements of each theater of war are distinct. The nature of

USE OF TACTICAL AND STRATEGIC INTELLIGENCE



alliances, adversary military capabilities, and political and military objectives are different within each theater of war. A theater commander may require access to the assets of the strategic intelligence community to support peacetime or wartime campaign planning. However, the immediate focus of the NCA may be toward political and military developments in another theater of war.

An operational level of war intelligence perspective is necessary if the peacetime and wartime campaign planning objectives of the operational-level commander are to be realized. This is due to the demands on the strategic intelligence community and the focus of tactical intelligence. Operational level of war intelligence is defined as that intelligence which is required for the planning and conduct of campaigns within a theater of war. At the operational level of war, intelligence concentrates on the collection, identification, location, and analysis of strategic and operational centers of gravity. If successfully attacked, they will achieve friendly political and military-strategic objectives within a theater of war.

Operational level of war intelligence focuses on the intelligence requirements of theater, army group, field army, or corps commanders. The echelon focus at the operational level is situationally dependent. It reflects the nature of the theater of war itself. It shows the political and military objectives of the combatants. The echelon focus also reflects the types of military forces which can or may be employed. The planning considerations of the tactical commander will be principally "military" in nature. However, the campaign-planning considerations of the operational-level commander will incorporate political, economic, psychological, geographical, and military factors on a grand scale.

Within a theater of war, joint and combined military forces are employed to realize the political objectives set forth by the NCA. Realization of political objectives within theater requires the defeat of those strategic and operational centers of gravity which permit an adversary alliance to maintain the momentum of a campaign effort and necessary political support. Identification, targeting, and defeat of these centers of gravity is contingent upon an IEW perspective and system which takes account of the peacetime and wartime planning imperatives of an operational-level CINC. Certainly the demands on the strategic intelligence community in a time of war will limit the ability of theater staffs to access these systems. If the focus of operational responsibility is a theater command, the EAC MI brigade will generally provide intelligence support to that command. Access to national-level systems will be maintained by the EAC intelligence center (EACIC). However, the bulk of the all-source intelligence analysis—and the performance of operational-level IPB functions—to satisfy the requirements of theater staffs and commanders, will be performed by the theater J2 with the support of the J2 staff and the EACIC. And because of the focus of intelligence at the tactical level of war—evolving battles and engagements and the rapid dissemination and exploitation of combat information and tactical intelligence—intelligence produced at this level, if not properly screened, could well overwhelm theater and subordinate staffs and distract them from their necessary operational-level perspective.

Five IEW tasks are performed at the operational level of war: situation development, target development, electronic warfare, security and deception, and indications and warning (I&W). Situation development or IPB at the operational level of war involves four functions: theater area evaluation, analysis of the characteristics of the theater AO (geographical, political, economic, industrial, communications, analysis of the entire theater of war to discern the operational impact of significant

regional features on the conduct of both the friendly and adversary campaign effort), threat evaluation, and threat integration. The theater J2 will discern the political and military designs of the adversary and specific objectives within theater. He will determine the time required to realize these objectives and target areas of interest (TAIs) keyed to strategic and operational centers of gravity. The J2 follows this enemy activity by continuously developing and refining situation, event, and decision-support templates.

Target development at the operational level involves the identification of those high-payoff targets (HPTs) as part of the theater C^3CM strategy or operational engagement scenario that, if attacked, will lead to the defeat of centers of gravity. EW or joint and combined EW at the operational level will interface with other joint and combined destructive systems in the context of the theater C^3CM strategy. OPSEC measures and the theater deception strategy will be incorporated in the theater campaign plan.

The fifth IEW task, I&W, involves the continuous development and refinement of regional or theater-based indicator lists. These allow operational-level intelligence staffs to determine changes in the political, military, economic, and diplomatic behavior of an adversary. This allows the theater commander to better anticipate and understand NCA actions which may lead to the decision for military involvement.

Theater-based all-source intelligence analysis is necessary for a theater commander and the NCA to avoid strategic surprise. The Worldwide Indications and Monitoring System makes this possible.

High-intensity conflict in a theater of war follows when the powers involved fail to adhere to long-standing rules of behavior. A theater J2 staff learns the adversary's political designs. The information is gleaned during the performance of the second and third functions of operational level of war IPB (analysis of the nature of the theater of war and threat evaluation). This yields a broad picture of how an adversary alliance could be expected to fight, and for what objectives.

The purpose of tactical intelligence operations is to obtain and provide decision makers reliable information about the enemy, weather, and terrain as quickly and completely as possible. The results are an essential basis for estimating enemy capabilities, courses of action and intentions, and for planning friendly operations. Intelligence seeks to discover the type, strength, location, organization, and behavior of enemy forces; their direction and speed of movement; and their intentions. It includes information about the weather and terrain within the operational area and their effects on friendly and enemy operations.

Order of battle (OB) is an integral part of intelligence concerning the enemy. OB is the identification, strength, command structure, and disposition of personnel, units, and equipment of a military force. Complete OB data is seldom provided commanders. Instead, commanders are provided estimates and analyses based on collected OB information and other intelligence data. OB is significant at both strategic and tactical levels. At the tactical level, it is used to determine enemy capabilities, weaknesses, courses of action, and intentions. Weather and terrain information and intelligence are vital to making these determinations.

Weather intelligence results from the analysis of the effects of weather on both friendly and enemy operations. It is used by almost every element of a combat force. Commanders must be prepared to exploit favorable weather conditions and minimize the adverse effects.

Terrain intelligence results from an analysis of the effects of the terrain on friendly and enemy operations. It orients on the capability to move, shoot, and communicate. The terrain is analyzed in terms of its military aspects.

Terrain conditions have a profound effect on both friendly and enemy operations. The terrain within specific battlefield areas is analyzed in terms of the military significance. Terrain analysis is performed to determine the specific terrain conditions, based on current and projected weather conditions, under which enemy and friendly

forces must move, shoot, and communicate. Information about the enemy, weather, and terrain, once processed and reported, is intelligence. Intelligence is used at all levels of command—strategic, operational, and tactical echelons—to plan major campaigns and battles.

The commander, through the G2 or S2, directs the intelligence effort. Based on knowledge of the enemy, weather, and terrain, the G2 or S2 develops intelligence requirements to support the commander's concept of operations. He establishes priority intelligence requirements (PIR) or information requirements (IR). The PIR and IR, shown below, are the basis for intelligence collection and production.

PIR are the highest-priority intelligence requirements, and must be personally approved by the commander. Normally, PIR are enemy capabilities, enemy courses of action, or characteristics of the battlefield which could decisively impact on the commander's tactical decisions. There is no prescribed limit to the number of PIR, but there should be a clear priority among them.

IR provide intelligence which is less critical to the commander's tactical decisions, as well as information to support the needs of other functional areas and subordinate units of the command.

Collection is the process of gathering information from all sources. Collection operations are guided by the commander's requirements and are facilitated by use of the collection plan and the IPB data base.

Processing is the phase of the intelligence cycle whereby information becomes intelligence. Information from all sources is evaluated, correlated, and analyzed to produce an all-source product.

INTELLIGENCE AND INFORMATION REQUIREMENTS	
PRIORITY INTELLIGENCE REQUIREMENTS	**Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision making.**
INFORMATION REQUIREMENTS	**Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander.**

Dissemination and use of intelligence is the last and most vital phase of the intelligence cycle. Usable information and intelligence are rapidly disseminated to those who need it without waiting for additional information or further processing.

Most information is used in the development of intelligence. Much of this information, however, can be used immediately for fire, maneuver, or ECM. If raw data can be used for fire, maneuver, or ECM as received, with no interpretation or integration with other data, it is called combat information. Targeting data is a subset of combat information. Dissemination of combat information must be expedited and, at some echelons, a separate channel for routing combat information is established.

Combat Information: Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements.

Once raw data is validated, integrated, compared, and analyzed, it becomes intelligence. In other words, the distinction between intelligence and combat information is in how the information is handled and used. If information must be processed and analyzed, especially if integration with other data is required to produce usable data, it is intelligence and not combat information. Information may be both combat information and intelligence, but in sequence.

Intelligence generally falls within specific categories. These categories include—

- Human intelligence (HUMINT).
- SIGINT
- Imagery intelligence (IMINT).
- Scientific and technical intelligence (S&T intelligence).

HUMINT includes all information derived through human sources. Tactically, it is represented by interrogation of enemy prisoners of war (EPWs) and civilian detainees, translation of captured enemy documents, long-range surveillance operations, patrols and observation posts (OP), liaison with local military or paramilitary forces and the local populace, and, most importantly, reports from friendly troops.

HUMINT has the potential to discover the most guarded secrets to include enemy intentions. It generally has an advantage in the collection of less precise and quantifiable information requiring qualitative and value judgments. Examples of the most lucrative HUMINT targets are those which involve plans and intentions, deliberations and decisions, research and development, doctrine, leadership, training, and morale.

HUMINT sometimes suffers in timeliness of information. However, much overt tactical HUMINT is immediately exploitable as combat information. The ideal HUMINT sources are privy to decisions and intentions before they are widely communicated or acted upon—a requirement most other sources cannot meet.

SIGINT is the product resulting from the collection, evaluation, analysis, integration, and interpretation of information derived from intercepted electromagnetic emissions. It is divided into communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). COMINT and ELINT are used at all levels. COMINT consists of information derived from intercepting, monitoring, and locating the enemy's communications systems. ELINT is obtained by intercepting and studying the enemy's noncommunications signals, such as radar, and locating these emitters. FISINT is the technical information and intelligence information derived from intercept of electromagnetic emissions, such as telemetry, associated with the testing and operational deployment of foreign aerospace surface and subsurface instrumentation. By analyzing each signal, information is developed about the emitter and its user. Integration of this information with that from other resources provides accurate targeting data and a basis for determining enemy intentions.

IMINT is derived from radar, photographic, infrared, and electro-optic imagery. This imagery is analyzed by imagery analysts (IAs) to identify and locate enemy activity, installations, and equipment. Side-looking airborne radar (SLAR) has the capability to detect vehicle movement over large areas, has a stand-off capability of considerable distance, and has the capability to be digitally downlinked to the ground for in-depth analysis. Photographic imagery analysis is very accurate and is susceptible only to more sophisticated camouflage, concealment, and deception techniques. Positive identification of equipment can be made from photographic imagery in most cases. Infrared needs no light to image and best results are obtained at night. The system has the capability to detect individual thermal images and may have applications in a low-intensity conflict (LIC). Electro-optic systems are similar to photographic systems but differ in that the image is a digital recording which can be manipulated to obtain optimum results.

The disadvantages of IMINT depend on the limitations of the various sensors. Weather is a factor to some extent for all of the sensors. Radar, since it is an emitter, is susceptible to jamming. Photography is limited, for all practical purposes, to daylight hours and has no near-real time capability. Time sensitive requirements may be missed due to the time required for aircraft return and film downloading and processing. Infrared sensors require the aircraft to fly at low altitude (less than 3,000 feet) and directly over the target. Electro-optic systems suffer most of the limitations photography does, though not to the same extent. Some correction can be made to the image by digital enhancement.

There are systems considered to be IMINT systems that do not produce a hard copy image, nor are they utilized by IAs. These are ground surveillance radars (GSRs) and night observation devices.

Each of these intelligence disciplines is vulnerable to enemy deception, human error, and equipment malfunction. Intelligence producers must be aware of these vulnerabilities, and confirm reported information with another source whenever possible.

S&T intelligence is that intelligence concerning foreign technological developments and the performance and operational capabilities of foreign materiel which now or eventually may have a practical application for military purposes. Although principally a function of EAC and department-level MI units, S&T intelligence contributes significantly to fulfilling the intelligence requirements of tactical units. Typical S&T intelligence targets at tactical levels include enemy equipment and facilities. Tactical units must rapidly evacuate captured equipment and personnel of S&T intelligence value to S&T intelligence units, who exploit them in support of tactical and strategic requirements.

Combat information and intelligence may result from actions taken within any of the categories previously described. For example, SIGINT may provide a key element of intelligence that tells the commander when the enemy will attack. IMINT may provide the strength of the attacking force. HUMINT may provide knowledge of where the enemy will strike. Taken separately or in isolated increments, it is unlikely that a complete picture of the battlefield can be developed. However, the integration of these bits of intelligence with other information provides a composite that allows the commander to "see" the battlefield. The composite picture of the battlefield is the result of intelligence from all sources.

Intelligence can never be complete. Limited time and resources, battlefield confusion, and enemy deception all work to degrade the quality and quantity of intelligence. To provide the best intelligence possible, intelligence collectors are concentrated on the most valuable indicators of enemy intentions and targets of the highest value.

In order to plan intelligence collection and decide which collector to task, the targets for intelligence collection are divided into categories. These categories allow us to match the activity (such as movement along a section of road) with the collector capable of detecting it (such as SLAR). Most enemy units simultaneously

fall into more than one category, but it is the activity as a specific type of target that will answer a specific intelligence need. The four categories of targets are—

- ☐ Movers: Moving elements of the enemy force.
- ☐ Emitters: Communications and noncommunications systems.
- ☐ Shooters: Weapons and weapons systems.
- ☐ Sitters: Stationary targets.

The detection, location, and tracking of movers are important in identifying enemy patterns of activity. Movement patterns help locate enemy concentrations of combat power, defensive positions, lines of communication (LOC), key installations, and movement of reserves. By tracking movers in the area of interest, precise times and locations for attacking HPTs may be determined. Movers are often lucrative targets themselves.

Since virtually every unit on the battlefield uses communications and noncommunications emitters, electromagnetic emissions are especially lucrative sources of information and intelligence. Analysis of electromagnetic emissions provides—

- ☐ Targeting data for fire support, offensive air support, and jamming systems.
- ☐ Intelligence collected through the interception of enemy communications.
- ☐ Intelligence derived from traffic analysis and cryptanalysis.
- ☐ The identification and location of weapons, units, and systems through the detection and location of both communications and noncommunications emitters.

Shooters include all direct- and indirect-fire weapons and missile systems. Generally, shooters are located through their projectiles after they are fired or launched. However, missile systems, due to their nuclear, biological, and chemical (NBC) capability, must be located and destroyed as movers, emitters, or sitters before they can be fired.

Sitters are fixed or semi-fixed targets such as enemy command posts (CPs) and service support facilities. They may include other, more mobile targets which have stopped and are not shooting or emitting. Such targets may include forces in an assembly area, weapons in ready or firing positions but not firing, and other such targets. Sitters can be critical to enemy operations, and their destruction can severely degrade enemy combat power over the long term. Identification and location of sitters may provide indicators of enemy intentions.

Information collected against each of these targets may be used as combat information, as direct targeting data, and as intelligence.

The resources available to each commander for use against the four target categories are listed in the following table. Additionally, an enemy unit may be an emitter-shooter-sitter or emitter-mover target at the same time. Therefore, more than one resource may be employed against the same target.

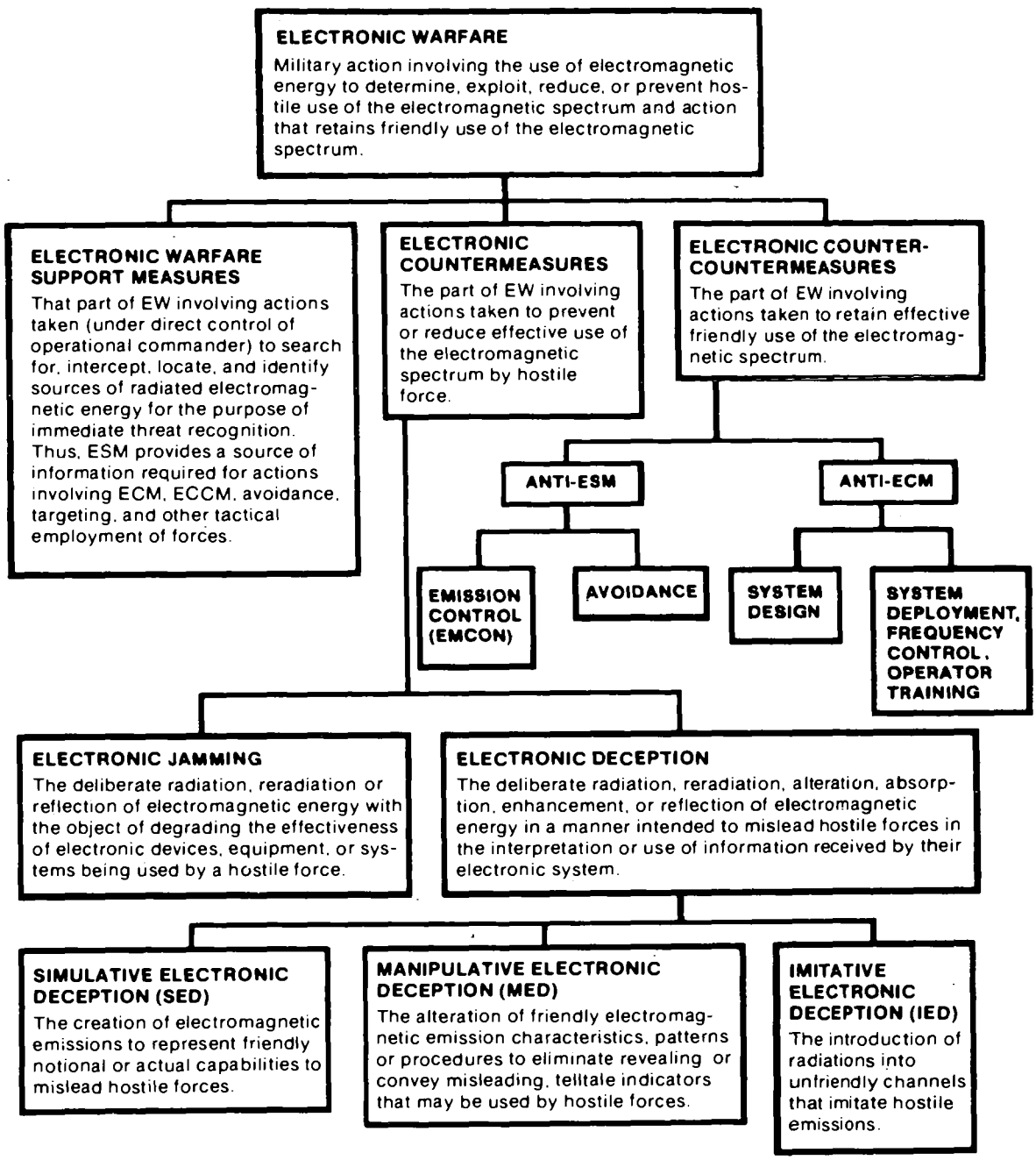
COLLECTION RESOURCES

RESOURCES	TARGETS			
	MOVERS	EMITTERS	SHOOTERS	SITTERS
Interrogators	X			X
Controlled Sources	X			X
Counterintelligence		X		X
Reconnaissance	X		X	X
Troops	X		X	X
HF/VHF Intercept		X		
VHF/UHF Intercept		X		
Multichannel Intercept		X		
NONCOM Intercept		X		
SLAR	X			
Photo	X		X	X
Infrared	X	X	X	X
Airborne Radar (USAF)	X			X
GSR	X			
Weapons Locating Radar			X	
Technical Intelligence Units	X	X	X	
Special Operating Forces	X	X	X	X
Fire Support Team (FIST)	X		X	X
Combat Aviation	X		X	X
Battlefield Surveillance (Artillery) Radar	X			X
Air Defense Radar	X			

ELECTRONIC WARFARE

EW is an essential element of combat power. Its contribution lies in exploiting enemy weakness, protecting friendly freedom of action, and reducing security and communication vulnerabilities. A modern military force depends on electronics for command and control of forces and employment of weapon systems. Because of this dependence on electronic devices, both friendly and enemy forces are vulnerable to action which can reduce the effectiveness of these devices or gain intelligence from them. EW functions are shown below.

ELECTRONIC WARFARE FUNCTIONS



Defensive EW cannot physically destroy a target. It can, however, when integrated into the overall concept of the operation, confuse, deceive, delay, disorganize, and target the enemy. When other considerations are equal, victory may go to the force that uses EW most effectively. EW is a command responsibility. It is a combat power element having two facets—offensive and defensive.

Offensive EW is the employment of EW to disrupt or deny the enemy's effective use of their electronic systems. It consists of ESM and ECM. An understanding of its functions is essential for planning, managing, and directing the employment of EW.

ESM include essentially the same functions as SIGINT but are focused on the more immediate requirements of the tactical commander. The relationship of ESM to SIGINT is similar to the relationship of combat information to intelligence. Tactical resources performing SIGINT may perform ESM simultaneously with, or as part of, SIGINT missions. The primary difference between ESM and SIGINT is how the information is used. Generally, ESM is a producer of combat information that can be used for ECM, fire, maneuver, or threat avoidance with little systematic analysis or processing. SIGINT, however, requires separate processing to produce the desired product. ESM and SIGINT are mutually supporting. Information collected through ESM may be processed to produce SIGINT. SIGINT is essential to support EW.

ECM includes electronic jamming and deception. One function of jamming is to degrade the enemy's combat power by denying effective operations in the electromagnetic spectrum. Another function of jamming is to reduce the signal security (SIGSEC) of enemy operators and thereby gain information through ESM. Jamming may be subtle and difficult to detect, or it may be overt and obvious. It can be accomplished from both ground and aerial platforms.

Electronic deception is integrated with and extends and reinforces tactical deception operations. It requires unique and specific training and planning and must be well controlled if it is to be effective. The objective of electronic deception is to deceive enemy forces through their electronic systems.

Defensive EW are those actions taken to ensure friendly effective use of the electromagnetic spectrum. Commanders rely on electronic emitters for C^2 and for many other critical battlefield functions. The first priority of defensive EW is to protect these emitters from enemy detection, location, and identification. CPs or weapon systems cannot survive on the modern battlefield if they can be located through their electronic emissions. Friendly use of the electromagnetic spectrum and the location of critical installations and systems are protected through ECCM.

ECCM are protective in nature and are planned around the commander's mission and concept of the operation. Planning begins with the identification of essential friendly emitters and sensitive communications that must be protected. Friendly electronic emitters, signatures, and profiles are evaluated based on their vulnerability to enemy REC and SIGINT capabilities. ECCM are then planned to overcome these vulnerabilities.

ECCM are closely related to SIGSEC. The primary difference lies in the type of information that is protected from enemy collection. ECCM protect friendly emitters from enemy detection, location, and identification. ECCM conceal electromagnetic signatures or deceive the enemy as to the location and identification of the emitter. SIGSEC, on the other hand, protects the information that is transmitted through friendly C-E systems from enemy exploitation. Many operator techniques may serve as both ECCM and SIGSEC measures.

ECCM, under the direction of the C-E officer, begin with training and are executed by every element of the combat force that uses or is responsible for the use of electronic emitters. The responsibility for ECCM starts with commanders and extends to supervisors and operators at all levels. Techniques for reducing friendly vulnerabilities to enemy REC efforts are directed through the Communications-Electronics Operating Instructions (CEOI),

Communications-Electronics Standing Instructions, standing operating procedures (SOPs), and other instructions.

The effectiveness of defensive EW is continually assessed to validate existing ECCM and to determine the necessity for additional measures. Defensive EW is fully described in FM 24-33.

COUNTERINTELLIGENCE

CI is that activity intended to detect, evaluate, counteract, or prevent hostile intelligence collection, subversion, sabotage, international terrorism, or assassination conducted by or on behalf of any foreign power, organization, or person operating to the detriment of the US Army. It includes the identification of the hostile multidiscipline intelligence collection threat, the determination of friendly vulnerabilities to that threat, and the recommendation and evaluation of security measures. CI operations are conducted to support OPSEC, deception, and the rear operations.

Support to OPSEC

OPSEC is the process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. CI supports OPSEC by focusing on the hostile intelligence threat and assisting in developing methods of defeating that threat. In coordination with the operations staff, CI personnel help to compare friendly force profiles against enemy collection capabilities. The comparison results in the identification of friendly vulnerabilities that must be protected. OPSEC measures are then developed to counter the enemy HUMINT, SIGINT, and IMINT threat at each level.

Support to Deception

Deception complements OPSEC and is, therefore, of significant interest to CI operations. Deception operations are conducted to mislead the enemy as to our intentions and capabilities, thereby causing a reaction that assists us in achieving our objective. Battlefield deception is deliberate action to achieve surprise on the battlefield. It is directed against enemy commanders and intelligence and target acquisition systems. Deception operations must be fully coordinated with affected friendly forces (adjacent and echelons above and below). Extreme caution must be exercised to prevent compromising the deception plan during coordination.

CI plays a vital role in both deception planning and operations. CI support to deception falls under three basic areas:

- Determination of enemy intelligence capabilities or efforts that may be susceptible to deception.
- Production of deception recommendations.
- Confirmation of the effectiveness of deception operations.

With their knowledge of the enemy's multidisciplined intelligence threat, CI personnel of corps- and division-level battlefield deception (BAT-D) cells are in a position to recommend offensive deception techniques to mislead the enemy. Once a deception operation is initiated, its effectiveness is evaluated through CI analysis and offensive tactical CI operations. CI personnel, in coordination with intelligence and deception analysts, monitor the effectiveness of deception operations through the screening and interrogation of EPWs, line crossers, and refugees. They also analyze combat information and all-source intelligence reports.

Support to Rear Operations

The threat to the rear area is a key consideration when planning or conducting tactical operations. Both division and corps rear areas are highly vulnerable to intelligence collection and combat operations conducted by conventional and unconventional enemy forces. CI operations, conducted in these areas, provide the intelligence needed to plan rear operations in order to preserve our freedom of action.

CI supports rear operations by determining the enemy's intelligence capability against rear operations and recommending countermeasures to those vulnerabilities. CI also identifies, exploits, and neutralizes rear area threats, such as agents, saboteurs, enemy sympathizers, and special purpose forces. CI support to rear operations begins

before hostilities. Peacetime operations identify potential agents and sympathizers that pose a threat to rear area security. IPB is used to determine most likely avenues of approach to rear area targets. OPSEC measures are developed to protect or minimize the threat to the target. During hostilities, CI elements continue to assess the vulnerabilities of rear area bases and base clusters and to recommend countermeasures. They provide early warning of threats to rear area operations and assist with the neutralization of such threats.

SYSTEM ELEMENTS

The IEW system includes combat, combat support, and CSS elements. While MI units provide dedicated IEW support, all units in the combat force, by virtue of their mission, capabilities, and AOs, have an implied mission of collecting and reporting information. The IEW mission is accomplished through the integrated efforts of all elements of the force. In turn, every element relies on support from the IEW system to accomplish its mission.

Maneuver units are among the best eyes and ears of the command. Individual soldiers and leaders provide a great deal of real-time targeting and combat information. Maneuver units conduct patrols, capture prisoners and documents, operate OPs, and observe enemy forces with whom they are in contact. They report information about the activity of enemy first-echelon forces, patrols, and reconnaissance elements.

Combat information and targeting data collected by maneuver units are normally used by the collecting units to engage the enemy. Pertinent information is introduced into the IEW system by the S2 or G2 of the collecting unit. By collecting and reporting information, maneuver units support the IEW effort. They, in turn, receive intelligence, EW, and CI support from other elements of the system.

Field artillery units provide the IEW system with valuable information about enemy activity. The tactical fire direction system (TACFIRE) has markedly enhanced the field artillery capability to collect, analyze, and disseminate targeting data. Organic target acquisition resources provide information concerning the enemy through—

- Visual observation.
- Combat observation lasing teams.
- Moving-target-locating radars.
- Weapon-locating radars.
- Aerial observers.

Artillery fire support teams (FIST) operating with maneuver units are a major source of targeting and other combat information.

Combat information and targeting data are exchanged constantly between operations and intelligence staffs and the field artillery TOC. This exchange takes place through the FSEs at each tactical echelon. FM 6-121 describes field artillery target acquisition.

Cavalry is a combined arms combat maneuver force mounted in ground and aerial vehicles. It constitutes the primary reconnaissance capability at corps and division. It is uniquely organized, equipped, and trained to find the enemy and prevent the friendly main body from being engaged under adverse circumstances. Conducting these tasks, cavalry elements provide the IEW system information about terrain, effects of weather on the terrain, and the presence or absence of the enemy. In turn, cavalry relies heavily on the IEW system for support to plan and accomplish its mission. FM 17-95 describes cavalry operations.

Air defense artillery (ADA) elements, equipped with target acquisition radars, provide surveillance information to the commander. In addition to organic target acquisition radar, ADA elements have direct access to and utilize long-range Air Force assets. They provide information about air routes into the friendly area and enemy air activity throughout the area of interest. ADA also provides statistical data about the destruction of enemy aircraft. FM 44-1 describes ADA operations.

Engineers routinely conduct route, stream, bridge, obstacle, air landing facility, and support area reconnaissance. Units operating with forward-deployed forces

provide intelligence, combat information, and other terrain data of value to the commander. Terrain teams at division, corps, and EAC provide terrain and trafficability studies and route overlays. Given sufficient time, overprinted maps may be produced by the corps cartographic company. FM 5-30 describes engineer reconnaissance, while FMs 5-146 and 21-32 describe engineer units and operations.

Army aviation resources, which range over the entire battlefield, have unique capabilities to observe both friendly and enemy activities. All aviation elements have the mission to observe the battlefield and report what they see. They provide combat information and intelligence about enemy locations, equipment, and movement. They also provide weather observations and information about the terrain. Aviation elements are particularly well suited to support OPSEC by detecting weaknesses in friendly camouflage and light discipline. USAF assets flying close air support (CAS) missions have a similar capability and may be contacted through the air liaison officer (ALO). FM 1-100 describes Army aviation operations.

Military police (MP) are responsible for good order and discipline and the collection, movement, and control of EPW. Alert and well-trained MP personnel can provide valuable information on prisoner behavior, rear area activities, and terrorism. FM 19-1 describes MP operations.

Combat service support (CSS) units make extensive use of road networks and provide valuable information about lines of communication, guerrilla activity, and weather and terrain conditions.

CSS and MP provide information useful in resource and refugee control and rear operations. FMs 100-10 and 55-40 describe supply and transportation operations.

Signal, ordnance, medical, and chemical units provide assistance in their technical areas of expertise by evaluating captured enemy materiel. Medical units provide intelligence by evaluating captured enemy medical materiel and also by providing information concerning the state of health of the enemy by medically evaluating selected EPWs, refugees, defectors, and escapees. Resulting information is processed and entered in the intelligence data base. Signal elements provide specific support to EW operations by processing and reporting enemy MIJI reports. FM 24-1 describes combat communications.

Civil affairs elements deal with people, equipment, and documents which are prime sources of valuable information. They significantly aid intelligence and CI operations by—

- Detecting and warning of sabotage activity.
- Detecting and reporting the transmission of information and supplies to enemy forces in the rear area, unfriendly partisans, and guerrillas.
- Locating and securing various records, periodical files, local publications, official documents, technical equipment, blueprints, plans, or other information of interest to intelligence analysts.

Psychological operations (PSYOP) units use intelligence as the basis for all operations. The objective of PSYOP is to modify the behavior and decrease the combat effectiveness of enemy soldiers and units. PSYOP intelligence personnel collect information on the attitudes, susceptibilities, and vulnerabilities of enemy forces. PSYOP units provide intelligence and in turn depend on the IEW system for intelligence to support their operations. FM 33-1 describes psychological operations in a combat environment.

ECHELON ARCHITECTURE

The IEW architecture includes the directors, coordinators, producers, and executors at each echelon of command. The following pages describe that architecture at each echelon from company to national level. It describes the capabilities for collecting and processing all-source information at each echelon against enemy mover, emitter, shooter, and sitter targets.

MANEUVER COMPANIES

Maneuver companies (and troops) form the broad base of the IEW system and are the reason for the existence of much of the system. Companies close with and destroy the enemy and, through direct contact, collect significant quantities of timely, accurate information of value to themselves and higher echelons. They, in turn, are supported by their parent battalions, brigades, divisions, and higher echelons.

Many of the information needs at this level are satisfied by resources assigned to the companies. Company commanders are concerned most about the enemy, weather, and terrain in their immediate areas—most of which they obtain through visual reconnaissance performed personally or by their subordinates. Targets are acquired and immediately attacked. If an enemy moves to the right or left, it is noted, and higher and adjacent units are notified.

In the course of collecting information for their own use, companies also collect information and capture exploitable sources of information of significant value to higher commands. This information may include indications of enemy morale, training, and combat effectiveness; the appearance of new weapons; and changes in tactics. Such information is passed to battalion for use and for processing and reporting to higher echelons. Captured enemy soldiers, equipment, and documents are evacuated for exploitation. The results of such actions may prove to be of significant value as either tactical or strategic intelligence.

Company commanders are the directors, coordinators, producers, and executors of company intelligence operations. They direct and coordinate company resources to satisfy company IEW requirements and those levied by the battalion. They request additional support from the battalion when required.

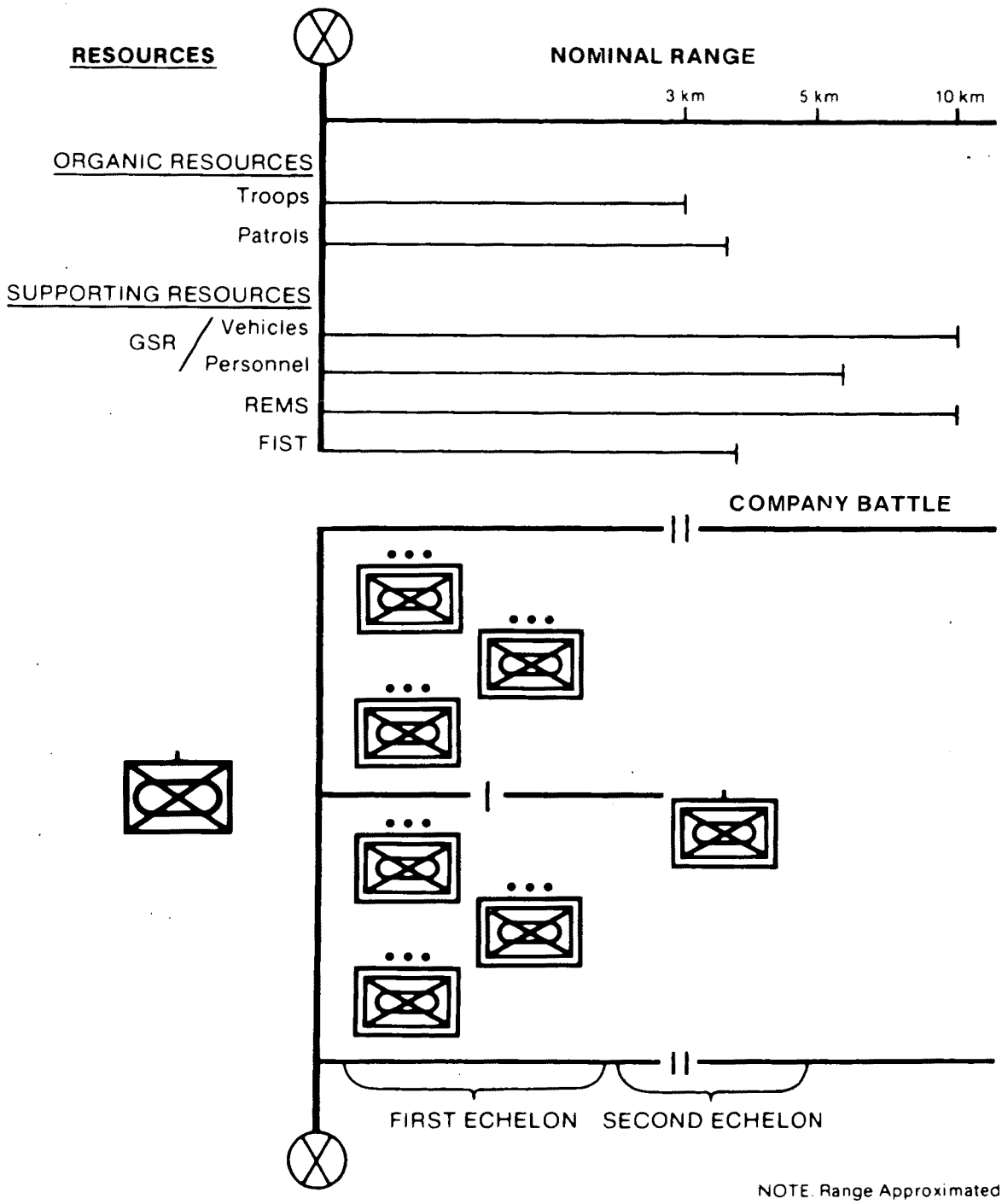
Company commanders need, almost exclusively, combat information which requires no processing or analysis. Any analysis required is done as a mental process by the commanders and subordinate leaders. More detailed processing requirements are satisfied by battalion and higher echelon staffs.

Company commanders direct the operations of company elements to satisfy IEW requirements. They direct the placement of organic sensors and those attached to, or placed in direct support (DS) of, their units. These organic sensors include low-level intrusion detection systems, while GSR may be attached to the company. Companies deploy patrols and OPs and task subordinate platoons to collect the information needed. Company EW requirements are very limited and are usually satisfied by higher echelons. However, the company may be tasked to orchestrate the use of company electronic emitters to support the deception operations of higher echelons. CI support to company OPSEC is provided as part of the support provided to the brigade and battalion.

The fire support team (FIST) located with the company is a critical collector of information of intelligence value. As they observe the battlefield and develop targeting data, this information is forwarded and analyzed to produce intelligence.

The resources available to the company commander for the execution of IEW requirements are depicted in the following illustration.

COMPANY RESOURCES



NOTE. Range Approximated

BATTALIONS

The battalion, like the company, relies primarily on combat information for the execution of the battle. However, its intelligence requirements exceed those of companies. The battalion receives information from the companies and other available collection resources which must be processed to a limited degree and passed to the battalion commander and brigade S2. The battalion, in turn, provides support to its subordinate companies. For these reasons, the battalion is provided a larger IEW capability than the companies.

Coordinators

The coordinators of battalion IEW operations are the battalion S2 and S3 supported by their respective staff sections and the BICC. As previously described, the S2 has staff responsibility for intelligence to include combat information, security, and CI. The S3 is responsible for EW and OPSEC.

At battalion level, the S2 is concerned primarily with coordinating combat information and reconnaissance and surveillance operations. He plans and coordinates the operations of resources organic to the battalion and to the MI battalion and field artillery resources supporting the battalion. Requirements which exceed the capabilities of these resources are passed to the brigade S2.

The battalion S3's responsibilities for EW, especially offensive EW, and OPSEC are relatively limited. Jamming and CI requirements are normally submitted to, and satisfied by, the brigade or higher headquarters.

Producers

The battalion BICC is the primary producer of intelligence. It consists of one officer and one enlisted analyst. Under the control and supervision of the S2, the BICC prepares the reconnaissance and surveillance plan, an informal collection plan, and other plans as necessary. It uses the maneuver companies, scout platoon, FIST, GSR teams, and other available and supporting units to collect information needed by the battalion. It forwards requests for information and support that are beyond the capability of battalion assets to the brigade or adjacent battalion BICCs.

The BICC provides the battalion with a limited analysis capability. It maintains a small intelligence data base and analyzes and integrates information to produce target data and intelligence. It promptly disseminates combat information to the battalion staff and to higher, lower, and adjacent units.

The battalion BICC is a key link in the intelligence system. It is the first processing element to receive front-line information about the enemy. It is a key element in expediting the flow of that information.

EW functions are completed as necessary by the S3 staff supported by the S2 section.

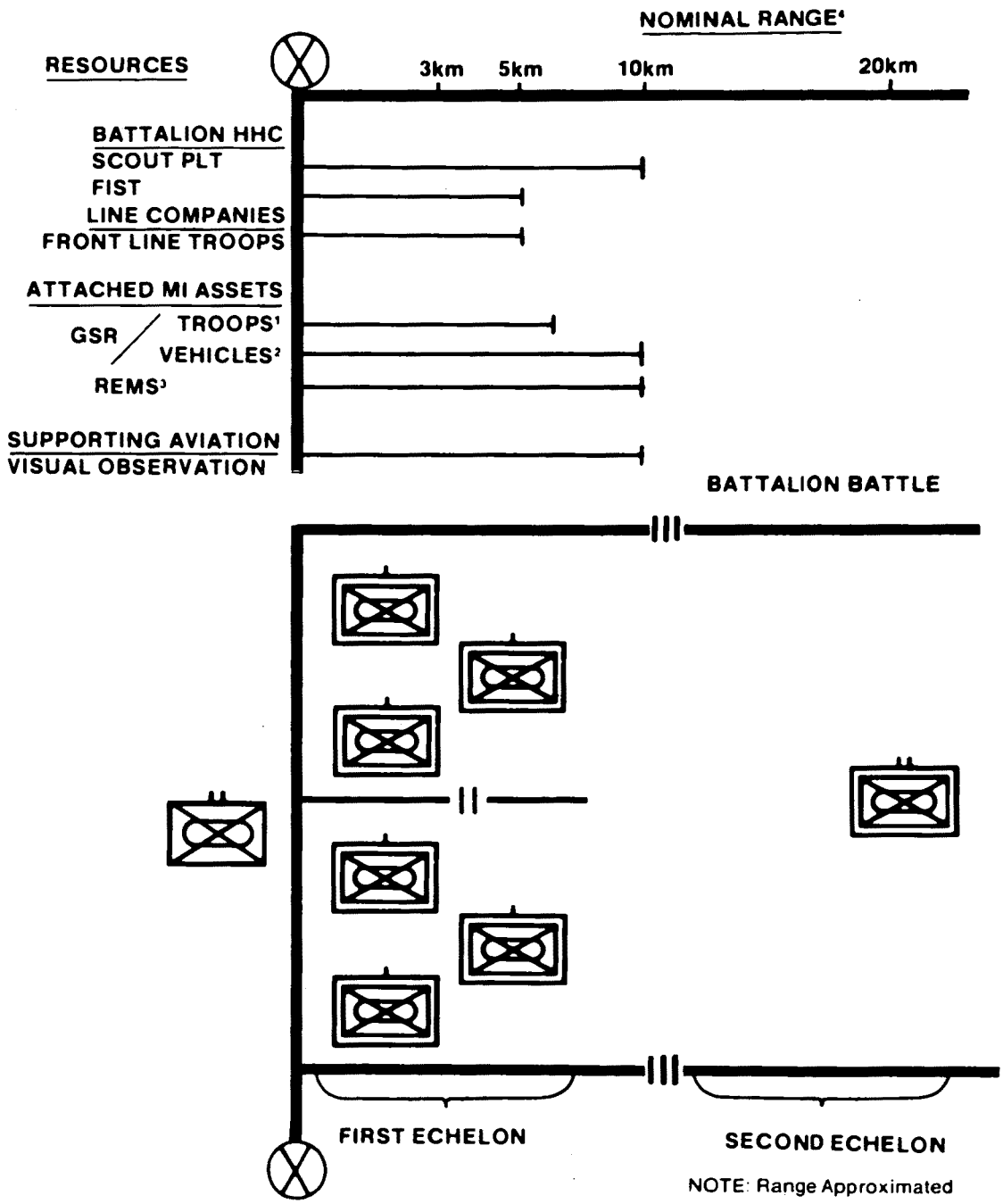
Executors

The executors at battalion level are the commanders of the companies and other units organic to, or supporting, the battalion. Tasking for reconnaissance patrols, GSR or remotely employed sensors (REMS) requirements, and observation missions are passed to the companies, scout platoon, or FIST. MI resources attached to, or supporting, the battalion may be allocated to the companies or held under battalion control. Those held at battalion are tasked directly by the S2 and S3.

Of the organic resources listed above, of primary importance to the S2 is the scout platoon. Although the S3 has the responsiblity for planning and directing the overall operations of the scout platoon, the S2 must recommend aggressive reconnaissance missions for it. Additionally, when the scout platoon is in a screening or security role, the S2 must ensure that collection missions are integrated into the operations of the scout platoon. These require constant active coordination with the S3 and the scout platoon leader.

The resources of the battalion are depicted in the following illustration.

BATTALION RESOURCES



1 - range is 1.5 km in light division

2 - range is 3 km in light division

3 - currently in airborne division only

4 - range for initial planning. Actual range depends on weather, terrain, enemy deployment, and location of enemy sensors.

BRIGADES

Divisional brigades have no organic IEW resources other than the staff sections and the brigade BICC. Still, the scope of brigade IEW operations is much greater than that of the battalion. To meet requirements, the brigade commander relies on subordinate battalions and support provided by elements attached from the division MI battalion and other division elements in the brigade's area. These normally include a field artillery (FA) battalion, an ADA unit, and combat engineers. MI support will normally include an IEW support element (IEWSE) to provide liaison between the brigade and the MI battalion. MI support will also include IEW assets deemed appropriate; these may be attached (such as a surveillance squad), placed in direct support (such as CI or interrogation teams), or task organized into an IEW company team (such as collection and jamming assets). An IEW company team may be DS to the brigade or GS to the division and deployed forward in the brigade sector. METT-T drives the stated command or support relationship.

The IEW requirements of the brigade still emphasize combat information; however, the need for intelligence, EW, and CI support is of nearly equal importance. Combat information is required for the operation in progress. Intelligence is required for planning operations for the next 12 to 24 hours. ECM is essential to reinforce fire and maneuver in disrupting the C^2 of enemy first- and second-echelon regiments. Additionally, the brigade is the focal point for CI support for itself and its subordinate battalions.

Coordinators

The S2 and S3 are the coordinators of IEW operations at brigade level. Working closely, these two staff officers identify the IEW requirements and coordinate actions to satisfy them.

As at battalion, the S2 is responsible for intelligence, security, and CI. Although CI requirements at brigade are limited, they do exceed those of the battalion and must be satisfied. Generally, the S2 identifies CI requirements and requests support through the IEW support element (IEWSE). The S2 is also responsible for supervising the brigade's BICC and for staff supervision of intelligence and CI operations supporting the brigade.

Brigade S3 responsibilities for EW far outweigh those at the battalion level. The brigade normally has EW resources deployed in its area. Therefore, the brigade S2 and S3, supported by the IEWSE and the BICC, identify the requirements and coordinate actions to satisfy them. Most importantly, the S3 integrates EW with fire and maneuver to maximize its effectiveness.

Producers

The producers at brigade include the BICC, the IEWSE, and the transcription and analysis (T&A) team of the supporting C&J platoon, if one is part of an MI team operating in DS of the brigade.

The functions of the brigade BICC are similar to those of the battalion. However, intelligence requirements, particularly analysis and production, are greater than those of the battalion. The brigade BICC coordinates closely with the IEW support element to ensure the intelligence effort between organic collection assets and supporting MI assets are effectively coordinated. The brigade BICC—

- Develops and coordinates the collection plan.
- Prepares and transmits tasking messages and requests for information to satisfy collection requirements.
- Develops data for the brigade S2's informal intelligence estimate.
- Develops and maintains the intelligence data base.
- Processes intelligence.
- Disseminates combat information and intelligence.
- Provides intelligence support to EW and OPSEC.

The IEWSE is provided to the brigade by the divisional MI battalion to coordinate the operations of MI elements operating in the brigade area. An IEWSE is deployed with each brigade, regardless of whether there are MI assets directly supporting the brigade or only GS MI assets in the brigade area. It acts as the primary link between the brigade TOC and the MI battalion. It provides the S2 and S3 information from MI elements, advice and assistance in planning the use of MI assets, and is the channel for passing brigade requirements to MI elements. It assists the S2 and S3 in identifying and requesting additional support from division, and if a company team is not formed, it coordinates the CSS needed by MI elements deployed in the brigade area.

The T&A team is part of the C&J platoon (voice collection platoon in light division) and is deployed as part of the platoon's headquarters. It performs selective scanning and gisting of voice intercepts recorded by collection teams. When necessary, extracts or complete translations of voice intercepts may be made. The team performs very limited analysis. It reports acquired combat information to the IEWSE and passes all intercepted information and technical data to the MI battalion's technical control and analysis element (TCAE).

The combined actions of the producers result in coordinated IEW support responsive to the brigade commander's needs. The BICC assists the S2 and S3 in planning and coordinating intelligence collection, EW, and CI support, and performs limited analysis for the production of intelligence. The analysis function, to include IPB, is limited at the brigade level. Brigade relies on division for IPB products and detailed all-source intelligence analysis.

Executors

The executors at brigade level include the battalions subordinate to the brigade, the DS FA battalion, air defense and engineer elements, and attached or DS MI elements.

The battalions perform reconnaissance, surveillance, and target acquisition (RSTA) operations, and report information to the brigade. These operations may be a result of normal battalion operations or specific tasking from the brigade. The resources used have been previously described in this chapter.

The nonorganic resources operating in support of the brigade, such as artillery, air defense (AD), and engineer units, also perform RSTA activities as they conduct their operations. Artillery radar locates enemy indirect fire systems, while their forward observers collect information on enemy units close to the FLOT. AD elements observe enemy aircraft and report information on their routes, numbers, and tactics. Engineer units observe the condition of terrain and obstacles, as well as enemy activities.

When diverse MI resources are deployed to support a brigade, the MI battalion commander may organize them into a DS IEW company team. This is done to simplify the C^2 and sustainment of these resources. When this type of IEW company team is formed, the team commander exercises C^2 of all MI battalion resources in the company team. The IEW company team is further described in Chapter 6.

The light division has organic interrogation teams which may be placed in DS of a brigade (as will the heavy division, if teams are attached from corps). A type interrogation team has five members. In DS at brigade, this team will concentrate on screening as many EPWs or detainees as possible. Those EPWs or detainees found to be knowledgeable and cooperative during the screenings will be given brief interrogations. All combat information obtained from these EPWs or detainees will be reported as rapidly as possible. The interrogation team can also translate documents and act as interpreters, but such activities are not their primary mission. The interrogation team is tasked by and reports to the brigade S2.

Ad hoc OPSEC evaluation teams, formed by the division G3, assist the brigade commander in evaluating OPSEC posture. These teams normally consist of unit personnel with expertise in the areas to be monitored and CI personnel. The teams advise of possible compromises and recommend adjustments to current OPSEC measures. They identify weaknesses and risks by examining unit and CP communications signatures and tactical deployment, determine vulnerabilities to enemy collection systems, and identify compromises of EEFI.

The surveillance squad is organic to the divisional MI battalion. It is task organized by the MI battalion in response to division tasking to meet brigade requirements. Normally, the GSR squad is attached to the brigade. The brigade may further attach the assets of the squad to maneuver battalions. The brigade may hold some teams under its control to support such missions as flank security. The squad leader is the executor for brigade taskings to teams held under brigade control, and also performs coordination, support, and supervision for parent unit responsibilities for teams further attached to battalions.

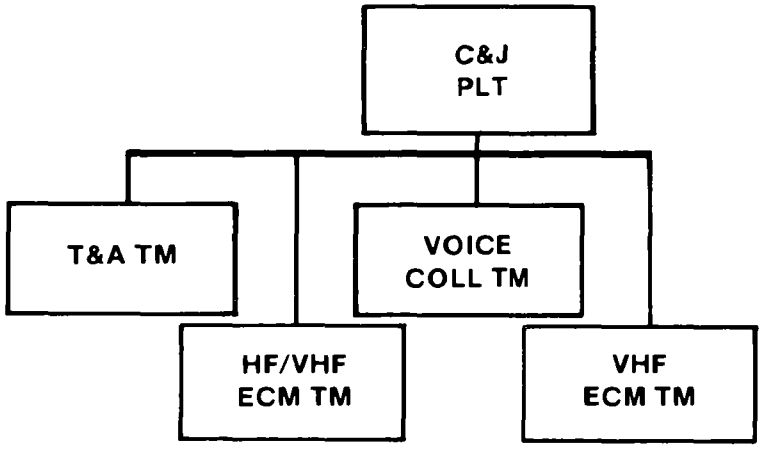
As part of a DS IEW company team, a C&J platoon may also be tasked to support the brigade. See the illustration above for the C&J platoon organization.

The platoon headquarters provides direction and control of the platoon. It is the focal point for tasking and reporting associated with platoon operations. It provides the necessary interface between the TCAE, the IEWSE, and the teams assigned to the platoon.

The T&A team and its functions were described earlier.

The voice collection team intercepts and summarizes high frequency (HF) and VHF voice communications. It also has a capability to provide line of bearing (LOB) information for intercepted transmissions. Recordings, intercept summaries, and LOB data are sent to the T&A team for further processing and dissemination.

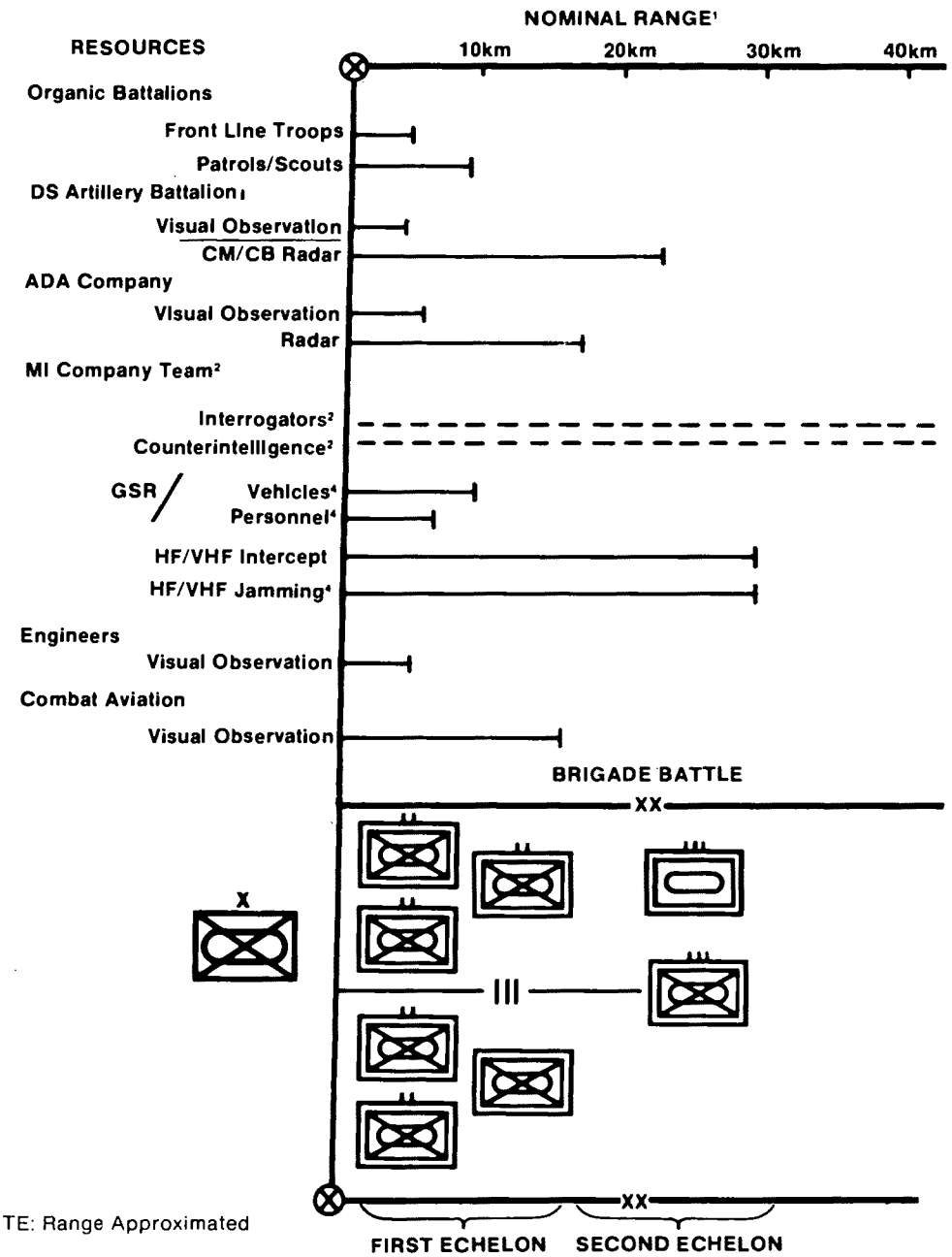
COLLECTION AND JAMMING PLATOON, MI BATTALION (HEAVY DIVISION)



The platoon is capable of jamming HF and VHF communications in close operations. In extreme situations, the orientation of team operations may be switched from attacking enemy communications to assisting friendly communications and deception operations. If critical communications are blocked by enemy jammers, the teams' high-powered equipment can be used to pass ***emergency*** messages despite enemy jamming signals.

In the light division, the C&J platoon is replaced by a voice collection platoon. This platoon may be deployed as part of an IEW company team in DS of a brigade, and consists of a T&A team, a voice collection team, and two low-level voice intercept (LLVI) teams. The T&A and voice collection teams

BRIGADE RESOURCES



NOTE: Range Approximated

1. Range for planning. Actual range depends on terrain, weather, enemy deployment, and location of friendly sensors.
2. Usually deployed in brigade area. May be GS to division or DS to brigade.
3. Range indefinite. Based on information obtained through exploitation of HUMINT sources.
4. GSR range is 1.5km for personnel and 3km for vehicles in light division.
5. No ground-based jamming in light division.

teams are structured as described above. The LLVI teams are equipped with manpacked ESM systems and are deployed on foot to augment the voice collection capability in the brigade area.

Further details on brigade and battalion IEW assets and operations are located in FM 34-80.

The resources available to the brigade, and their general capabilities, are depicted in the illustration on page 2-29.

DIVISIONS

Resources available at division include a substantial coordinating staff; a multidisciplined MI battalion; and various troop units, such as FA, ADA, engineer, and aviation. MI resource are allocated to the brigades and lower levels, data bases are maintained for complete intelligence analysis, and technical control is provided for ESM and ECM operations.

Coordinators

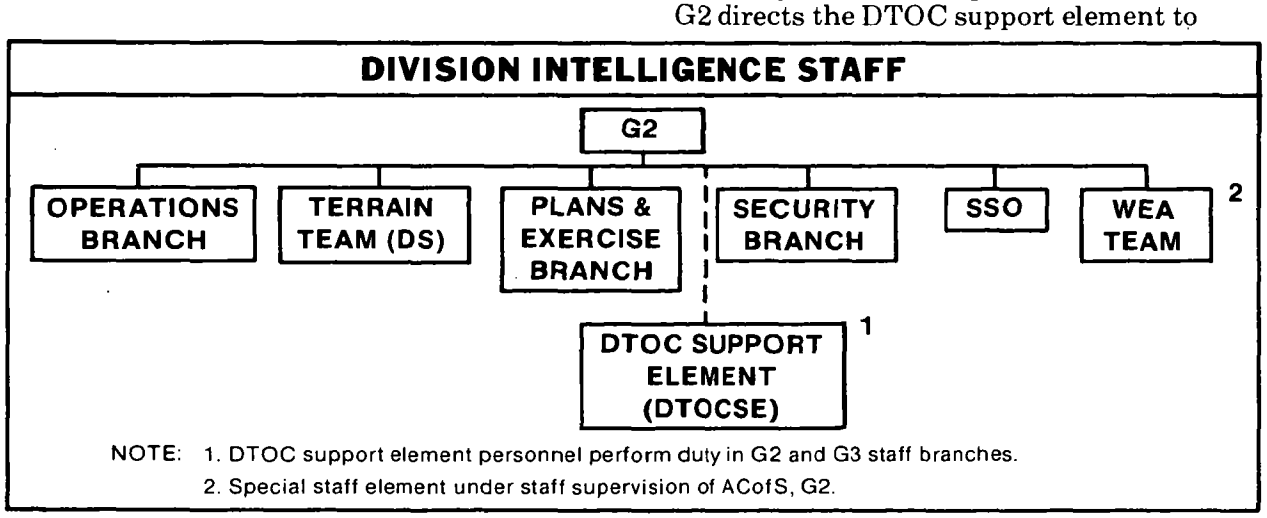
The coordinators at division are the G2 and G3, supported by their respective staffs. The G2 has staff responsibility for identifying requirements and planning and coordinating intelligence and CI operations. Formulation of division document and personnel security policy is also a G2 function. The G3 performs similar functions for EW and OPSEC.

There is no standard method for organizing the division intelligence and operations staffs. Each division staff is organized according to its own unique missions, threat, AO, and resources. A type organization for the division intelligence staff is illustrated below.

Within the DTOC, the intelligence staff functionally integrates with sections of the DTOC support element. G2 section branches coordinate closely with their counterparts in the DTOC support element to ensure that the intelligence effort is coordinated and satisfies the commander's requirements.

The G2 operations branch, based on G2 guidance, directs and coordinates intelligence, CI, division SSO, staff weather team, and the engineer terrain team operations. It coordinates the daily operations of the G2 staff within the DTOC, providing intelligence to the division commander, the other coordinating staff, and the special staff. It ensures that intelligence requirements to support current operations are satisfied, to include the dissemination of intelligence and combat information. It coordinates closely with the G3 operations branch and FSE to ensure that intelligence and CI operations are integrated with and support the commander's scheme of maneuver and the fire support targeting effort.

The G2 plans and exercises branch formulates and coordinates intelligence and CI for future and contingency operations by close coordination with intelligence personnel assigned to the G3 plans branch. The G2 directs the DTOC support element to



ensure that intelligence support to planning is provided, to include IPB and target value analysis (TVA).

The security branch develops division security policies and assesses the security status of the command. It coordinates with the CI analysis section of the DTOC support element for security assistance and CI support to OPSEC.

The G2 DTOC and tactical and rear CP elements may be staffed as separate branches or the necessary resources may be drawn from other G2 branches. The G2 element at the tactical CP provides the division commander and staff with the intelligence support required to conduct close operations. The element must be small and capable of continuous operations. The G2 tactical CP element coordinates closely with the G2 operations branch and DTOC support element at the division main CP to ensure that it is aware of current deep and rear operations as well as intelligence plans for future operations.

The organizational branches of the division G3 section operate in much the same manner as the branches of the G2 section. There are, however, several additional branches that are involved with IEW operations that deserve comment.

The EWS and OPSEC staff element augment the G3 for the management of division EW and OPSEC operations. The OPSEC staff element helps the G3 develop the command OPSEC program and supervise its implementation.

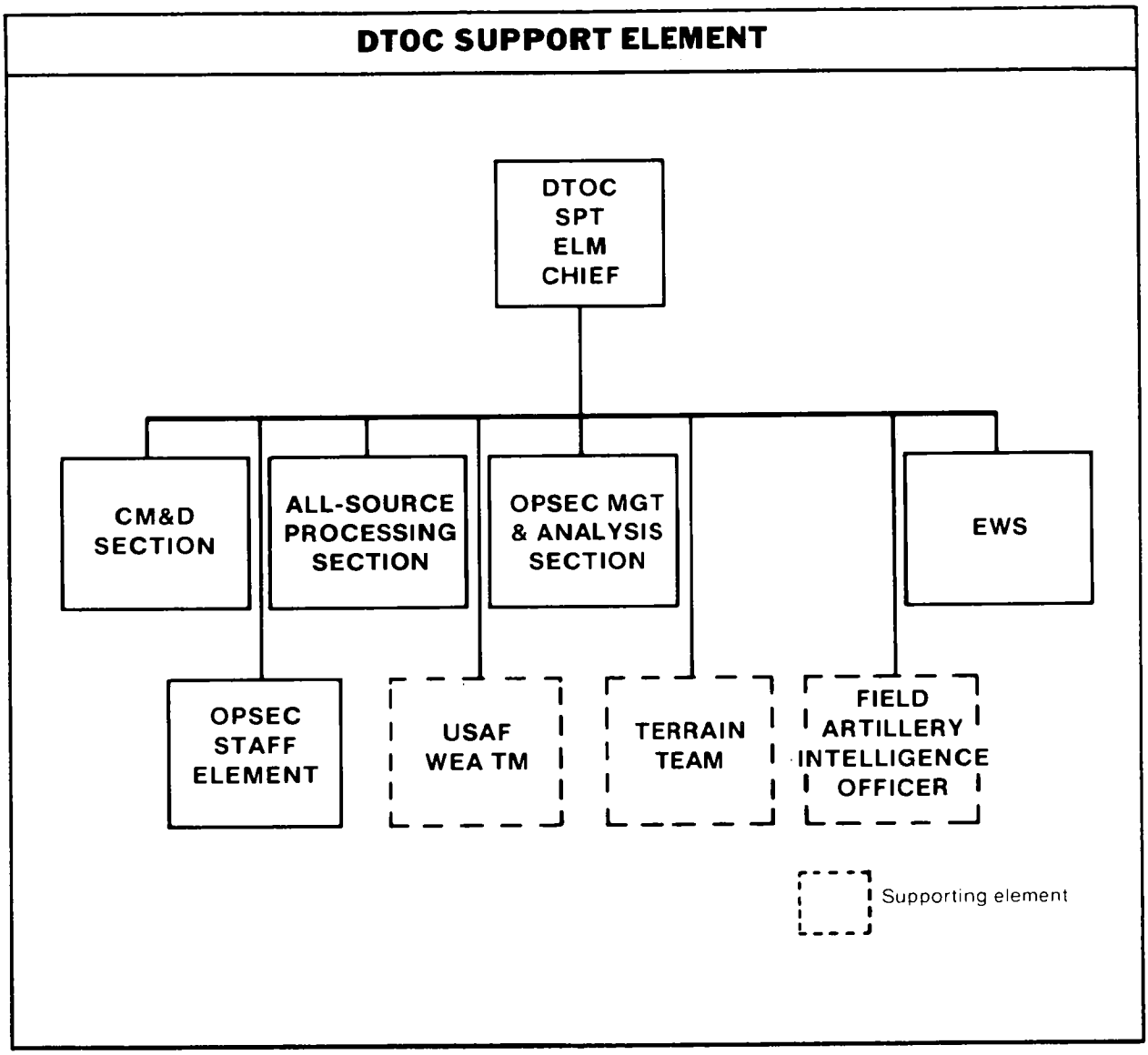
The EWS operates closely with the G3 operations and plans branches. This ensures that offensive EW is accurately coordinated into the division's operations, is compatible with the commander's PIR and IR, and supports his concept of operation. The EWS must ensure that EW operations are compatible with the fire support element (FSE) of the division staff. This functional integration between the FSE and the EWS is a continuous process and ensures that the efforts of these branches are not committed piecemeal to the battle. While security considerations may preclude a physical collocation of these two branches, close coordination between them is mandatory. The EWS, or personnel from the EWS, may be integrated within, or collocated with, the FSE to ensure that EW is integrated with lethal fire support. Ultimately, the EW effort must complement the fire support operations in the same manner as do close air operations or naval gunfire operations. This integration of EW and fire support will provide the commander with a total effort to support combined arms operations.

The BAT-D cell of the MI battalion is also a coordinator. It augments the G3 staff and coordinates with other elements with the DTOC, adjacent units, and higher and lower echelons, to ensure that deception operations are synchronized with division operations and plans. The overall deception plan developed by the corps BAT-D cell is integrated into the division operation by the division's BAT-D cell. The various "signature" teams of the cell then deploy within the division's AO to execute limited deception events. In this sense, the BAT-D cell is also an executor.

Producers

The DTOC support element is the producer at division level. The sections comprising the DTOC support element are shown in the following organization chart. The supporting weather and terrain teams and the field artillery intelligence officer (FAIO), while not part of the DTOC support element, collocate with, and function as, essential elements of the DTOC.

The DTOC support element augments the G2 and G3 staff sections for IEW operations in field and garrison situations. It supports the coordinating staff functions of estimating, recommending, planning, ordering, and supervising the execution of plans and orders. Generally, the G3 has staff supervision only of the EWS and OPSEC staff element which are collocated with the G3 section. The remaining sections are under the staff supervision of the G2. Formal tasking of sections is through the DTOC support



element chief; however, direct daily contact, to include informal tasking and direction between G2 staff elements and the DTOC support element sections, is essential.

In field operations, the DTOC support element normally deploys as a single entity and is physically collocated with the DTOC.

The collection management and dissemination (CM&D) section performs collection management for intelligence operations. Through collection planning it translates the commander's intelligence requirements into collection missions. Missions to be accomplished by MI assets are tasked to the MI battalion TOC. Missions for non-MI assets are passed to the G3 for tasking. The division CM&D forwards requests to the corps CM&D when they cannot be collected by division assets. The section disseminates combat information and intelligence throughout the command and to higher and adjacent commands.

The ASPS performs the division's IPB and brings together information from all sources to be analyzed, processed, correlated, and integrated into products to meet the commander's needs. It develops and maintains an extensive intelligence data base to include IPB and OB data and data

on enemy intelligence collection and air defense capabilities. It identifies gaps in the intelligence effort and cues the CM&D section for adjustments in the collection plan. The ASPS receives national intelligence products and sensitive compartmented information (SCI) from corps. This reliance on SCI requires close coordination with the SSO.

The CI analysis section, under the staff supervision of the G2, provides CI analysis support to OPSEC, rear operations, and deception. It supports the command's OPSEC program by working with the OPSEC staff element in the comparison of enemy collection capabilities with divisional profiles to identify vulnerabilities and OPSEC measures. It supports the rear operations mission by identifying and recommending taking action to neutralize level I and II threats. It supports deception planning by recommending deception techniques as an OPSEC measure or in support of battlefield deception operations.

The OPSEC staff element helps the G3 to fulfill OPSEC responsibilities. Working closely with the CI analysis section, it performs the OPSEC management functions necessary for development and implementation of the command's OPSEC program. In addition to these management tasks, the element's specific duties are to—

- Assist the G3 develop EEFI.
- Prepare the command's OPSEC plans and annexes.
- Provide input to and review deception plans and related publications and documents.
- Prepare and maintain the command OPSEC SOP.
- Develop, implement, and supervise command OPSEC training and education programs.

The EWS plans and coordinates EW operations to ensure that they are integrated with, and support, fire and maneuver. A primary function of the EWS is the management of ECM operations. It coordinates closely with the FSE to ensure that ECM and fires are fully integrated. ECM missions are passed to the MI battalion TOC for action. The section's functions include—

- Evaluating the vulnerability of enemy communications to ECM.
- Developing EW target lists which recommend targets for ECM to support current and planned operations.
- Recommending priority of effort for division jamming operations.
- Preparing EW estimates and annexes to operations orders (OPORDs).
- Coordinating ECM controls.
- Assisting the G3 in evaluating the effectiveness of jamming and electronic deception and recommending changes.
- Evaluating enemy REC efforts and recommending appropriate ECCM.

The FAIO, assigned to the FSE, operates with the ASPS in the DTOC. The FAIO assists in identifying targeting and target development requirements, and evaluates incoming reports to identify pertinent targeting data and facilitates its transmission to the FSE.

A terrain team from the EAC engineer topographic battalion is provided for DS terrain analysis to each division and corps. The teams normally collocate with the ASPS and also provide general support (GS) to subordinate units of the supported headquarters. They support the ASPS in its IPB function by providing a range of terrain products, to include IPB graphics. The teams maintain a close relationship with the parent EAC battalion for additional support beyond their capabilities.

The USAF weather team provides operational weather support to the division. Personnel from the supporting USAF Air Weather Service (AWS) unit staff this section. Common equipment, such as vehicles, generators, and communications gear is supplied and maintained by the division headquarters, headquarters company. Specialized equipment is provided by the AWS. The chief of the weather team, the SWO, is a division special staff officer. The weather team works closely with the ASPS and terrain team in the DTOC.

Executors

The principal executor at division level is the commander of the divisional MI battalion. He normally controls and directs the operations of all MI assets assigned, attached, or in support of the division. Other executors include all major elements of the division. Included are the commanders of the brigades; armored cavalry squadron; division artillery; engineer, ADA, and aviation units; as well as all other combat support and CSS units assigned to, or supporting, the division.

Within the MI battalion, the battalion TOC provides centralized management of organic and supporting MI assets. It operates under the direct supervision of the MI battalion S3, responding to IEW mission requirements received from the G2 and G3.

The battalion TOC consists of the S2 and S3 sections and the TCAE. The S3 section provides staff support to the S3 and manages and tasks intelligence and surveillance assets. The MI battalion S2 section maintains the current enemy situation and provides advice to the S3 to support tasking of all non-SIGINT EW assets.

The TCAE provides technical control of SIGINT and EW assets in response to tasking from the MI battalion S3. It maintains the enemy electronic order of battle (EOB), including SIGINT or REC threat and technical data bases. It analyzes and correlates ESM and SIGINT data from all sources to update the technical data base and produce SIGINT. SIGINT data is passed to the ASPS for correlation with other information and intelligence. Data on enemy SIGINT and REC is posted to the CI analysis and OPSEC staff elements for use by counter-SIGINT and deception personnel. The following chart shows the MI battalion (CEWI) (heavy division) organization.

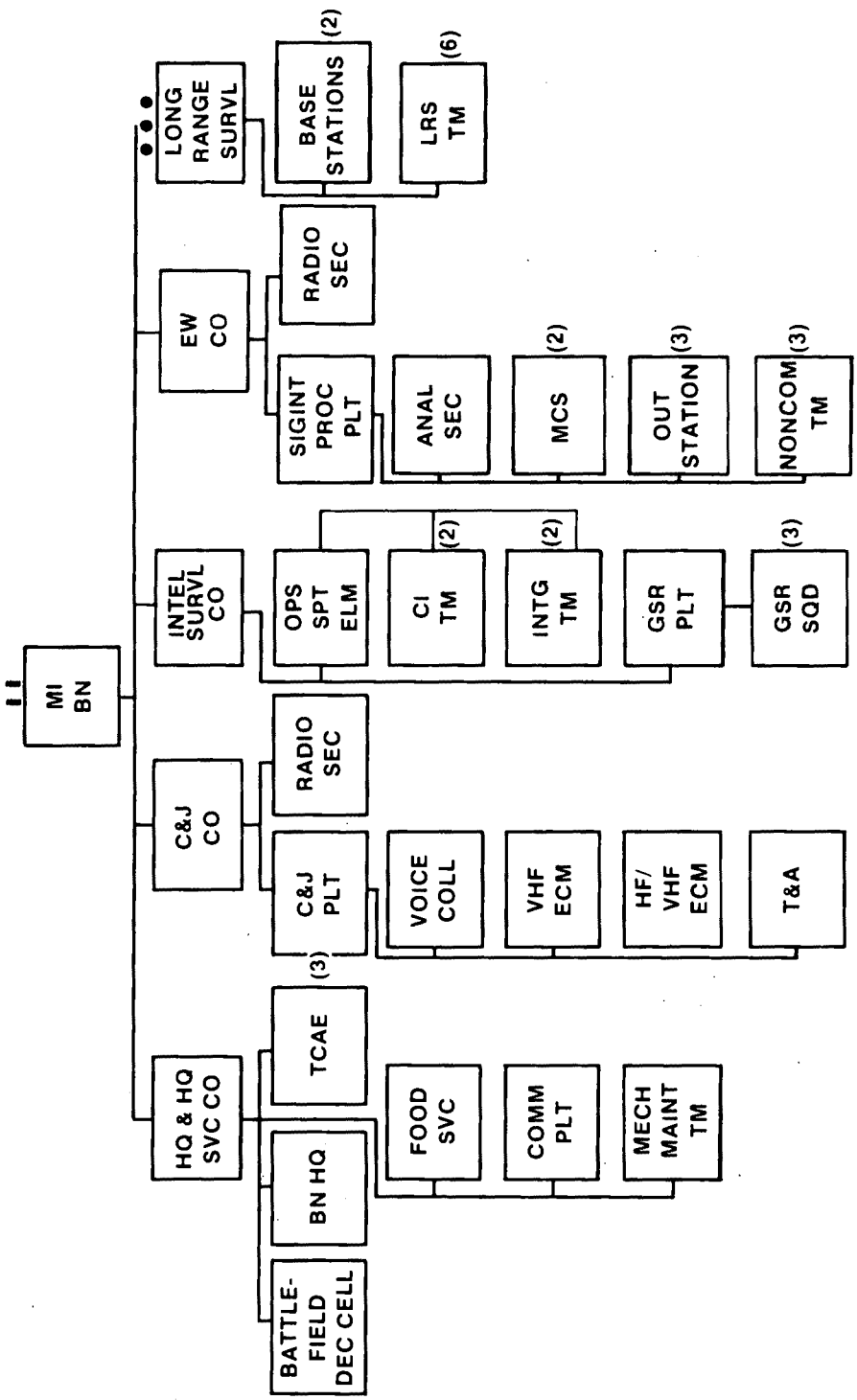
The C&J, EW, and intelligence and surveillance companies (MI) and the long-range surveillance detachment (LRSD) provide dedicated IEW resources to execute assigned IEW missions. The C&J company consists of three C&J platoons and communications assets. The C&J platoons were described earlier under brigade, since they are often part of an IEW company team placed in DS of brigades. The communications assets provide radio teletypewriter (RATT) systems which connect the C&J platoons to the TCAE. The EW company consists of communications assets and a SIGINT-processing platoon. The SIGINT-processing platoon includes the communications emitter locating system (TRAILBLAZER) and noncommunications intercept teams. These assets are normally employed in GS of the division. The SIGINT-processing platoon also contains an analysis team to provide limited processing of intercepted signals.

The intelligence and surveillance company provides CI, interrogation, and surveillance support to the division. It is organized with an operations support element and a GSR platoon. The operations support element consists of CI and interrogation assets which provide GS to the division. If CI and interrogation augmentation is received from corps, some elements may be placed in DS of a brigade. The surveillance platoon provides GSR support to the division. A surveillance squad normally supports each brigade. GSR assets may be placed in support of maneuver battalions and companies.

The LRSD provides collection in the division's areas of operations and interest. It performs passive surveillance to observe, evaluate, and report enemy dispositions, facilities, and activities. It also reports on terrain and weather conditions. Specifically, the detachment—

- Conducts long-range intelligence collection through reconnaissance and surveillance.
- Determines and reports the location, strength, equipment, disposition, organization, and movement of enemy forces and determines the location of high value targets (HVTs).

MILITARY INTELLIGENCE BATTALION (CEWI) (HEAVY DIVISION)



- ☐ Conducts damage assessments and NBC monitoring.
- ☐ Emplaces and uses unattended sensors and electronics intelligence, target acquisition, and designation equipment.
- ☐ Employs photographic and night image enhancement devices.
- ☐ Obtains information on possible drop zones (DZs) and landing zones (LZs) for airborne and air assault operations.

The MI battalion exercises OPCON over the QUICKFIX flight platoon, a GS asset, which is organic to the GS aviation company, combat support aviation battalion, aviation brigade. The QUICKFIX flight platoon provides three airborne COMINT and EW (QUICKFIX) systems to provide aerial communications intercept, locating, and jamming support.

In addition to organic resources, divisions may be supported by ECM and intercept platoons and CI and interrogation teams from corps. Each of these reinforces the organic capabilities of (and are controlled by) the MI battalion.

The ECM and intercept platoons have similar capabilities to those of the divisional MI battalion. The active component (AC) MI battalion (tactical exploitation (TE)) at corps can provide voice and noncommunications intercept and VHF ECM resources. When mobilized, the reserve component (RC) MI battalion (TE) provides voice and noncommunications intercept and HF and VHF ECM assets. Their augmentation expands the capacity to fulfill the division's SIGINT and EW mission.

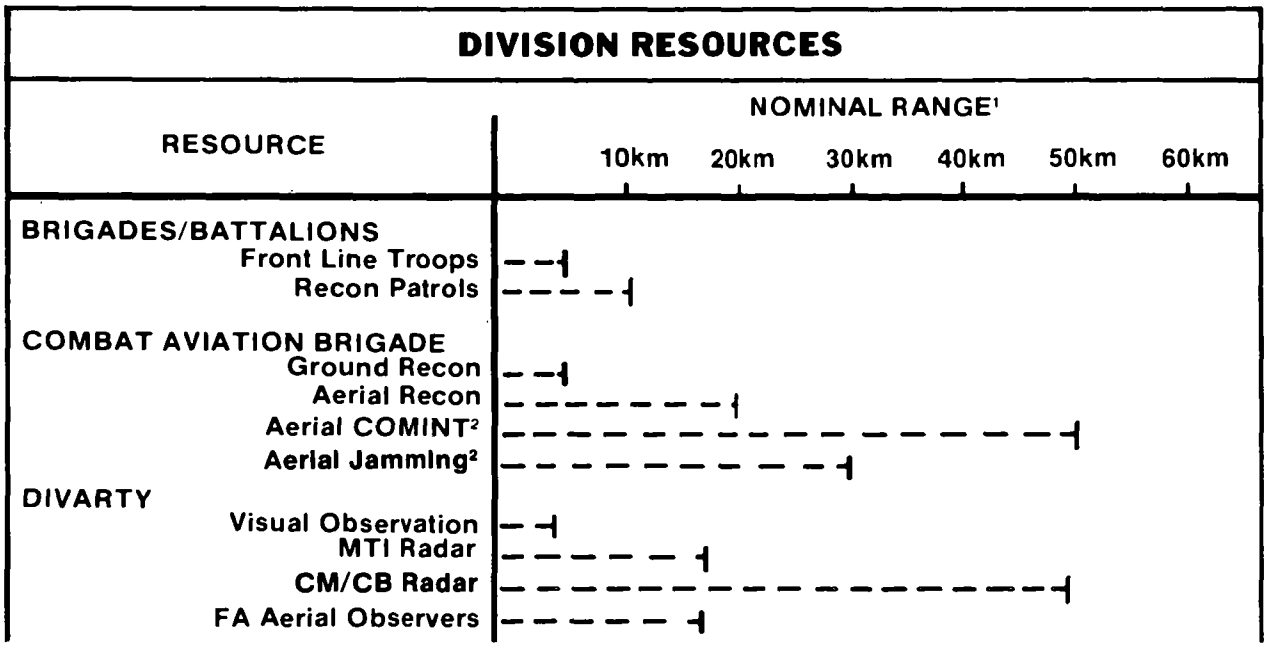
Interrogation and CI teams from the corps MI brigade may be placed in DS of the division or may be placed in a GS reinforcing role at the division main EPW collection point. These teams are provided by both the active and reserve components MI battalions (TE).

The MI battalions of the light, airborne, and air assault divisions have different structures, company titles, missions, and equipment. Details of their organizations and capabilities are explained in Chapter 2, FM 34-10.

A detailed description of division IEW assets and operations is also provided in FM 34-10.

The major resources of the division, to include their general capabilities, are summarized in the following illustration.

DIVISION RESOURCES



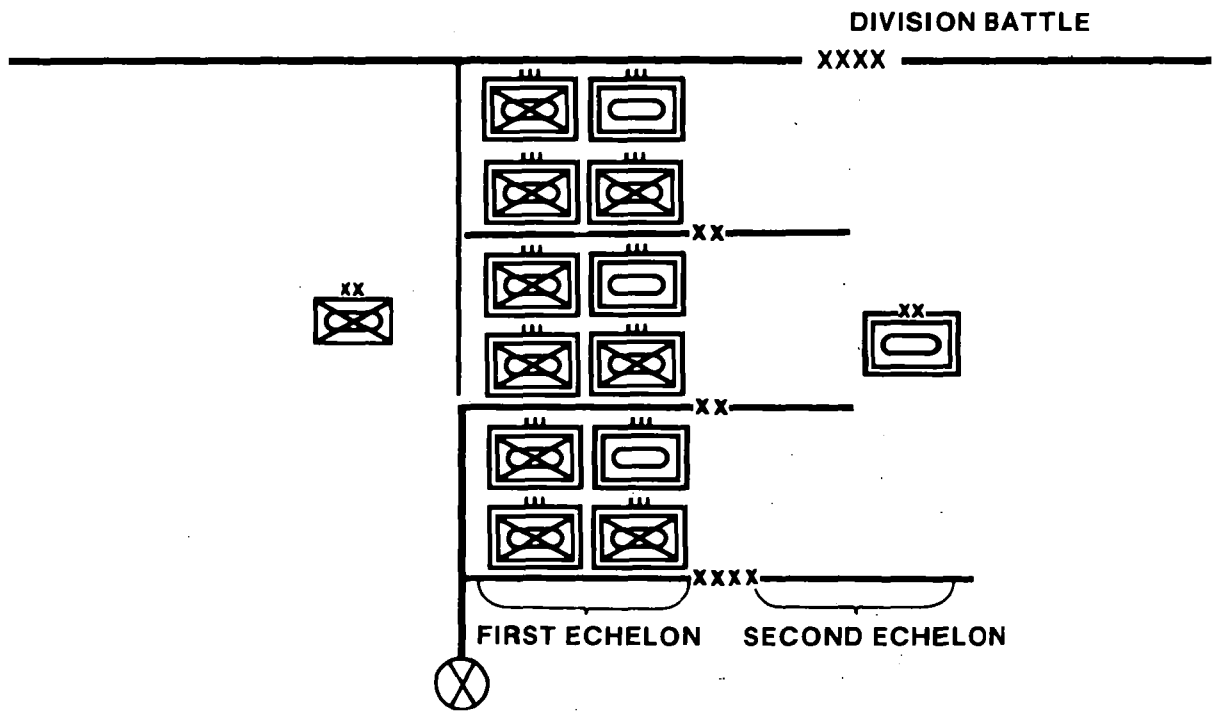
DIVISION RESOURCES (continued)

	10km	20km	30km	40km	50km	60km
ADA BATTALION						
Visual Observation	⊣	NOMINAL RANGE[1]				
Radar	⊣					
ENGINEER BATTALION	Within visual line-of-sight of assigned elements					
MP COMPANY	Within visual line-of-sight of assigned elements					
DISCOM	Within visual line-of-sight of assigned elements					
MI BATTALION						
Interrogation[3]						
CI[3]						
LRS Detachment					⊣	
COMINT				⊣		
ELINT				⊣		
Jamming				⊣		
Ground Survl Radar						
- Vehicles	⊣					
- Personnel	⊣					

1 Range for initial planning. Actual range depends on terrain, weather, enemy deployment, and location of friendly sensor.

2 Employed under OPCON of MI battalion.

3 Range indefinite; based on information obtained through exploitation of HUMINT sources.



ARMORED CAVALRY REGIMENT AND SEPARATE BRIGADES

The armored cavalry regiment (ACR) and separate brigade requirements are, to a degree, similar to those of the division. In fact, the multidisciplined MI company assigned at these levels is a miniature divisional MI battalion. Still, there are significant differences in the way the ACR and separate brigades are employed and in their respective MI companies.

Coordinators

The ACR and separate brigade coordinators of IEW operations are the S2 and S3; however, their responsibilities are expanded over those of their counterparts in the divisional brigades. In fact, the responsibilities and functions of the S2 and S3 of the ACR and separate brigade are very similar to those of the division G2 and G3. The major difference is that the scope changes with the size of the unit and the mission assigned.

MI BATTALION (HEAVY DIVISION) - MI COMPANY (ACR) COMPARISON

MI BATTALION	MI COMPANY
MI BATTALION TOC	MI COMPANY TOC
TCAE	TCAE
C&J COMPANY	C&J PLATOONS (2)
EW COMPANY	-
CI TEAMS (I&S CO)	CI TEAM (OPS SPT PLT)
INTG TEAMS (I&S CO)	INTG TEAM (OPS SPT PLT)
SURVL PLT (I&S CO)	SURVL PLT
COMM PLT (HHSC)	COMM PLT
MECH PLT (HHSC)	SVC PLT
DTOC SPT ELEMENT[1]	RTOC SPT ELEMENT[2]
QUICKFIX FLT PLT[3] (OPCON)	QUICKFIX FLT PLT[4] (OPCON)

1. In division HHC
2. In regiment HHT
3. In GS AVN Co, AVN Bde
4. In CBT AVN Sqn

Producers

The ACR and separate brigade coordinating staffs are provided a TOC support element from their headquarters troop or company. The TOC support element reinforces the S2 and S3 by providing collection management, all-source production, and EW planning and mission management. The TCAE carries out the SIGINT/EW management functions similar to the division's TCAE. OPSEC and CI support planning is carried out by the CI team of the operations support section. The CI team also conducts CI surveys. The modified table of organization and equipment of the ACR does not provide for an SSO. This duty position must be resourced by available personnel assets.

Executors

The executors of IEW operations in the ACR and separate brigade include the commanders of the MI companies, the subordinate squadrons or battalions, and the combat support and CSS units. The MI company commanders direct and control the operations of all IEW resources assigned, attached, or OPCON to the command. This section will deal primarily with the MI company (ACR), as the structure for RC MI companies to support the AC separate brigades has not been finalized.

The illustration on page 2-38 compares the MI battalion organization with that of the MI company.

The subordinate platoons and sections of the company perform functions very much like those of their counterparts in the divisional MI battalion. The service platoon provides essential supply, food service, and maintenance support to the company. The communications platoon provides personnel and equipment to operate the company's telecommunications and radio teletypewriter (RATT) facilities. The platoon also provides RATT support to the USAF weather team. The regimental tactical operations center (RTOC) support element is the nerve center for IEW support to the ACR.

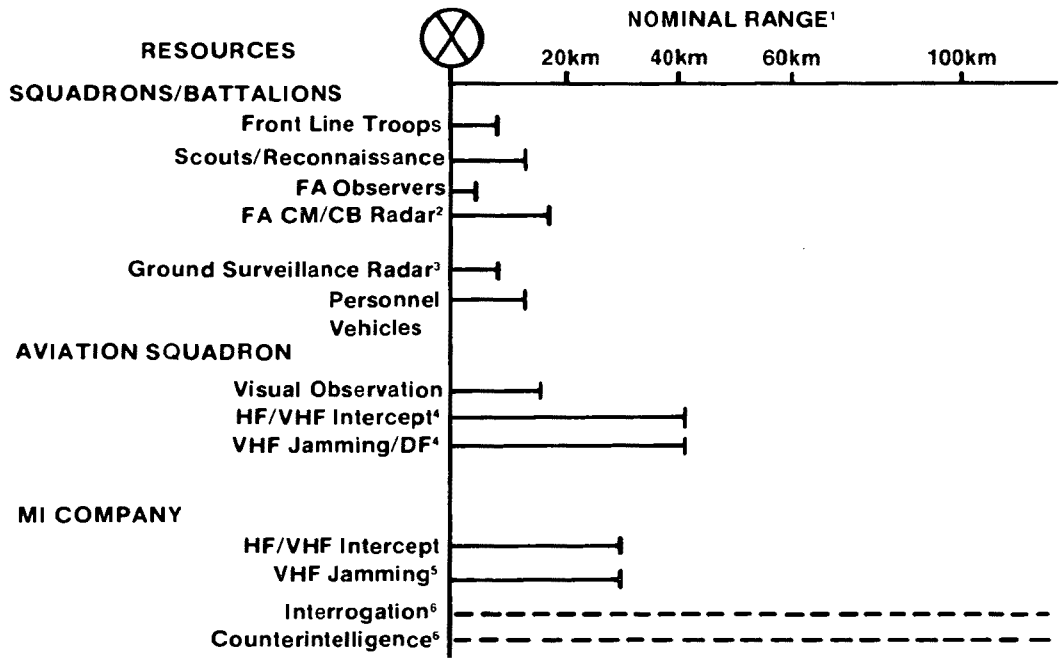
The surveillance platoon provides GSR for battlefield surveillance and early warning. The platoon is composed of three surveillance squads, each equipped with two radar sets. Normally, one squad is attached to each squadron. The platoon deploys them for early warning, combat surveillance, or target acquisition.

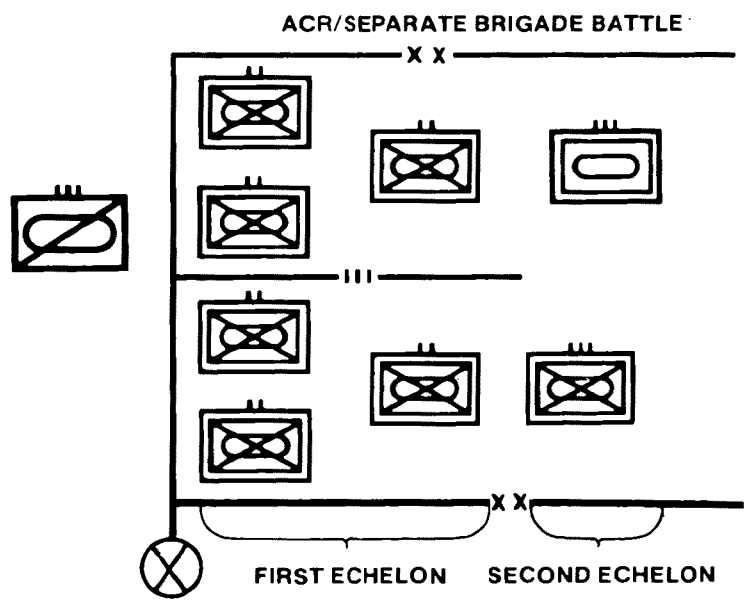
The C&J platoons are identical to the MI battalion's C&J platoons. The platoons provide voice collection and HF and VHF jamming. A T&A team is assigned to each to perform limited transcription and analysis. In the separate brigade's MI company, there are only voice collection assets—no jammers.

The operations support platoon provides interrogation and CI support. Both resources are used in GS of the ACR.

The QUICKFIX flight platoon (OPCON) provides airborne communications intercept, direction finding (DF), and jamming support. The platoon has its own maintenance personnel to ensure continued, reliable operation of the aircraft and related systems. This platoon is available only in the ACR, not the separate brigade. Further detail on ACR IEW assets and operations is in FM 34-35. The resources assigned to the ACR and separate brigade and their general capabilities are as illustrated on following page.

ACR/SEPARATE BRIGADE RESOURCES





1 Range for initial planning. Actual range depends on terrain, weather, enemy deployment, and location of friendly sensor.

2 TPQ-36 in FA battery organic to each squadron of ACR.

3 Attached to squadrons or battalions from MI company.

4 Employed under OPCON of MI company. Is in ACR only.

5 In ACR only.

6 Range indefinite. Based on information obtained through exploitation of HUMINT sources.

CORPS

The corps commander directs, coordinates, and supports the operations of divisions against the enemy first-echelon divisions and simultaneously directs the corps battle against enemy second-echelon divisions and armies. Although the corps needs some combat information, the primary requirements are for situation and target development. Corps EW requirements fall primarily within the realm of ESM. CI requirements are much greater than at lower echelons.

The MI brigade (CEWI) provides dedicated IEW support to the corps and its subordinate units. Most of the ground-based, and therefore short-range resources of the corps, are allocated in support of the divisions, ACR, and separate brigade. This includes the corps ECM resources which provide the capability to strike enemy forces in and just beyond close operations. The aerial assets comprise the source of most of the intelligence, target development, and poststrike assessment data generated at corps level. However, even these resources are unable to meet all corps requirements. The corps relies heavily on EAC, other services, and national agencies to supplement its collection capabilities.

Coordinators

As at division, the corps G2 and corps G3 are the coordinators of corps IEW operations. Although the scope of their responsibilities is greater because of the corps mission, their functions, organization, and responsibilities are similar to those of the division G2 and G3.

Producers

The MI brigade provides a corps TOC support element to reinforce the G2 and G3. Its basic organization and functions are similar to those of the DTOC support element with the addition of an IA section. The IA section provides imagery exploitation, advice, and assistance to the other sections of the corps tactical operations center (CTOC) support element. It also reinforces the capabilities of the IA section within the MI battalion (aerial exploitation). An additional IA section may be attached to the USAF tactical reconnaissance squadron supporting corps. The CM&D and ASPS at corps differ from those at division only in size and scope of activities. The MI brigade also provides a BAT-D cell to the corps G3, similar to the cell at division. It differs from that at division in that it consists only of planners and lacks the signature teams found at division.

The EW section reinforces the G3 by planning and coordinating EW operations, assuring that they are integrated with fire and maneuver. EW support of deep operations and C^3CM is vital to corps operations. The EW section works closely with the FSE to ensure ECM is integrated with long range fire in support of deep operations.

The CI analysis section reinforces the G2 with CI analysis support of OPSEC. A significant responsibility is to provide CI analysis support to the corps deception, C^3CM, and rear operations. The section also supports the divisions as required.

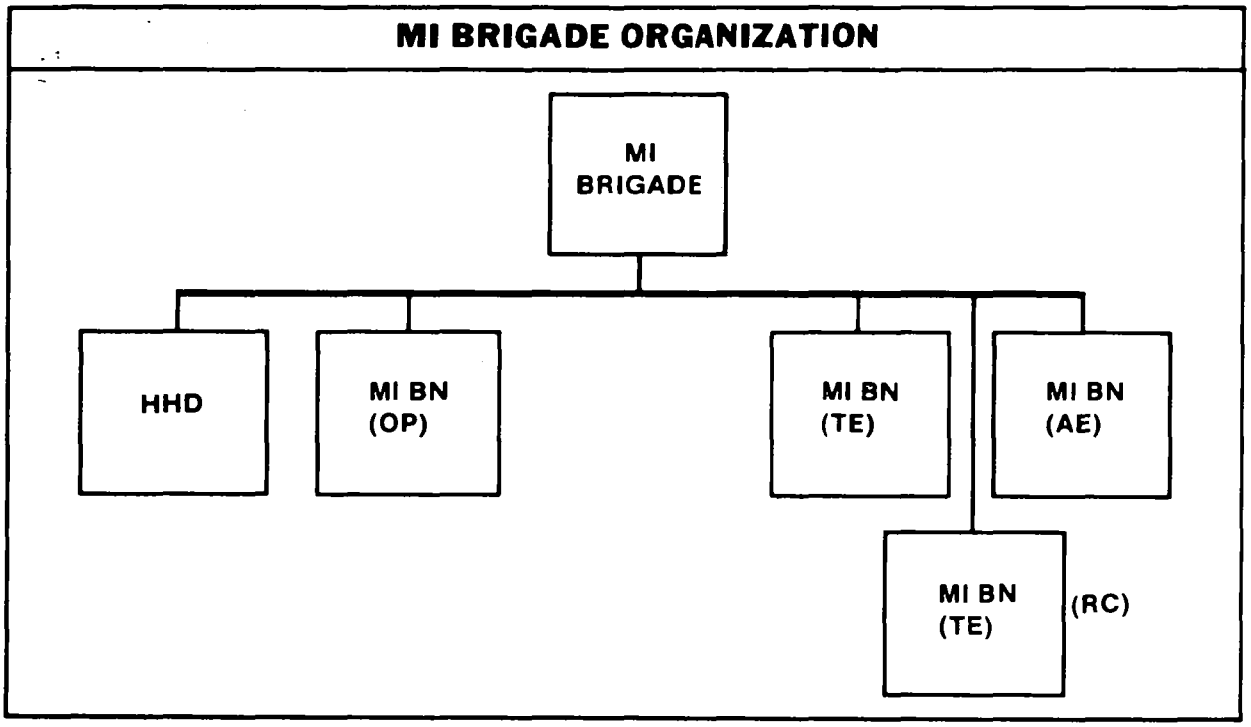
The OPSEC staff element reinforces the G3 by providing OPSEC planning and management support. Its duties are the same as the element at division.

Executors

The corps has an assigned multidisciplined MI brigade under the C^2 of the corps commander. The MI brigade TOC, consisting of the S2 and S3 sections and TCAE, provides centralized control of MI resources in support of the corps. It is reinforced by the IEW operations of other corps elements.

The TCAE interfaces with the TCAE of the divisions and the TCAE of the ACR to exchange technical control data. It also interfaces with the Army TCAE at EAC and with national systems to complete the vertical integration of technical data generated by tactical units with that produced by the National Security Agency (NSA).

The MI brigade is organized as shown in the following illustration.



The MI battalion (operations) provides the corps TOC support element to augment the corps G2 and G3, and the corps TCAE to provide technical control of corps SIGINT/EW assets. The corps TCAE also exchanges technical data with divisional TCAEs and the ACR TCAE. This battalion also provides the RATT assets for this TCAE to TCAE communications and also for corps CM&D to division CM&D communications.

The active component MI battalion (TE) has ground-based voice collection ECM, ELINT, CI, interrogation and long-range surveillance assets. These assets provide support to corps rear operations, and also augment the division and ACR and separate brigade capabilities. Its VHF ECM, voice collection, and noncommunications intercept platoons contain relatively short-range systems, and must be deployed far forward in the division areas. The battalion's CI and interrogation company provides a corps interrogation section and corps CI operations section which operate in GS of the corps. Its nine CI teams and eight interrogation teams may augment the limited assets that are organic to the divisions, as well as meeting corps needs. The battalion's long-range surveillance company is similar to the detachment at division. Its assets conduct passive surveillance operations in the corps area of interest.

Their capabilities are the same as those of the long-range surveillance detachment described under division.

The MI battalion (aerial exploitation (AE)) performs aerial surveillance and SIGINT. Its aviation company (AS) has OV-1D aircraft with SLAR and photographic sensors. The aviation company (EW) has GUARDRAIL and QUICKLOOK aircraft which perform COMINT and ELINT collection. The resources of this battalion are normally GS to the corps, but priority of effort can be weighted to one division or the ACR.

Reserve Component

The reserve component MI battalion (TE) will be assigned to the MI brigade and deployed with the active components of the MI brigade for training and upon mobilization. The mission of the reserve battalion is to augment MI brigade capabilities in support of the corps and subordinate units. The operational companies of the reserve battalion are described in the following paragraphs.

The operations and analysis company augments the active operations battalion. It provides sections to augment the CTOC support element headquarters, CM&D, and the CI analysis and OPSEC sections; analysis teams to augment both the CTOC and subordinate DTOC support elements; and augmentation to the corps TCAE.

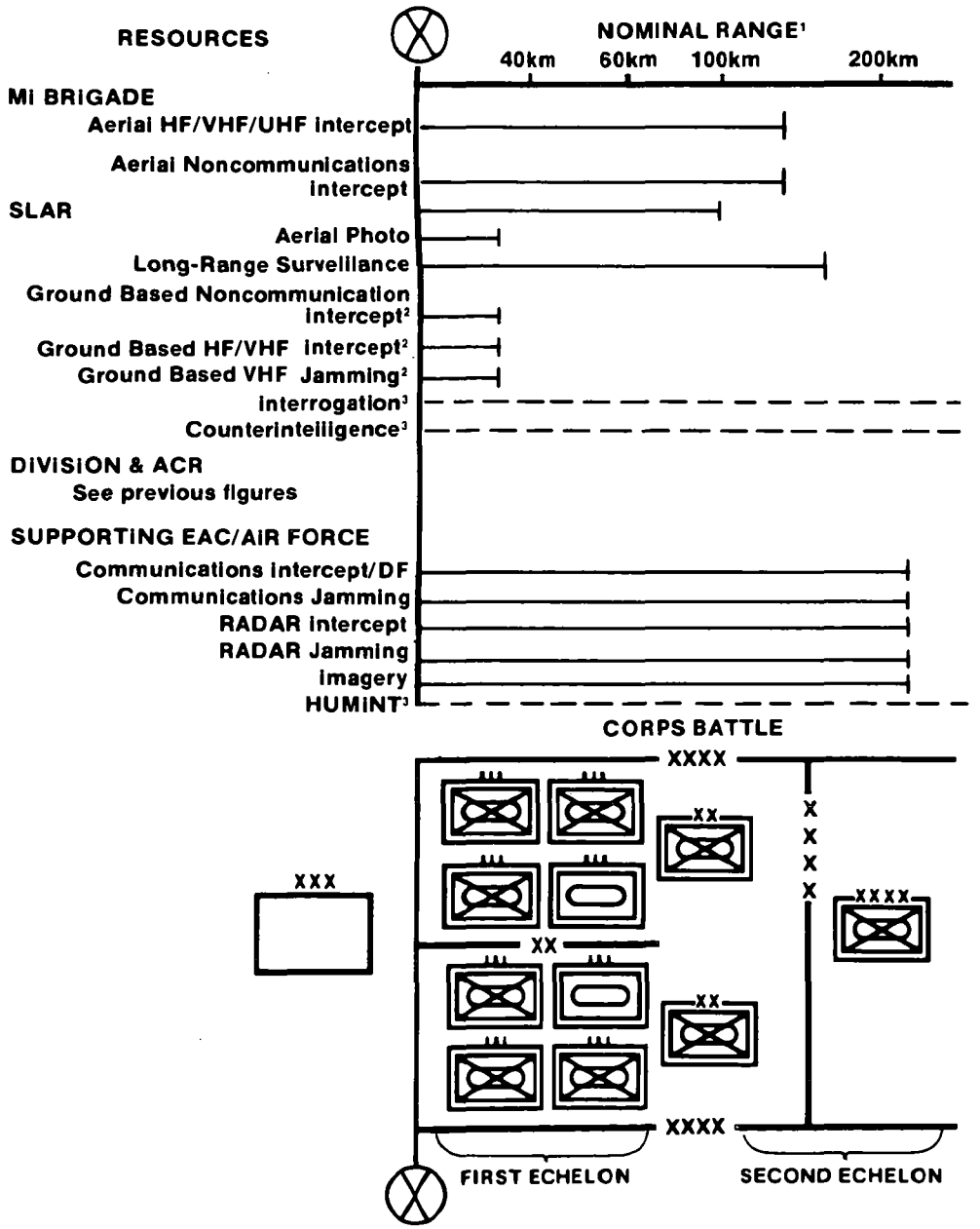
The CI and interrogation company provides teams of both CI and interrogation personnel to perform missions in the corps rear or for attachment to the corps' subordinate divisions.

The EW company (ECM) is organized with VHF and HF/VHF ECM platoons. These jammers must be deployed forward in the division areas due to range constraints, and will normally be attached to the MI battalions in the divisions. The noncommunications and voice collection systems in the EW company (collection) similarly will be deployed forward, attached to divisional MI battalions.

The training for the reserve MI battalion (TE) will require careful planning and coordination with the ACs of the MI brigade and the corps. To ensure common procedures and effective integration of the reserve unit, the periods of active duty training of the reserve MI battalion (TE) are closely coordinated with exercises and other training of active elements.

Corps IEW assets and operations will be described in more detail in FM 34-25. Corps resources are shown in the following illustration.

CORPS RESOURCES



1 Range for initial planning. Actual range depends on terrain, weather, and location of friendly sensor.

2 Normally attached to division or ACR MI units.

3 Range indefinite. Based on information obtained through exploitation of HUMINT sources. .

ECHELONS ABOVE CORPS

Commands at EAC may include allied army groups with operational command of US Army forces, allied regional commands, a US unified command, and separate US Army units assigned to NATO. They also may be a joint task force (JTF) headquarters in a contingency operation.

The Army IEW structure above corps supports US combat units, support units, and national agencies, and provides intelligence for use by joint and combined commands. It operates as an integral part of the US intelligence system and is capable of interfacing and functioning with allied military forces and host nations. IEW organizations and operating arrangements are tailored to fit the special needs of the commands involved. IEW support at EAC is keyed to providing support that is beyond the capabilities of corps and below MI units.

IEW operations at EAC are ongoing and conducted generally in the same way during peacetime as they would be in war. IEW organizations at EAC are organized for war. They may be modified for peacetime missions but are prepared for a rapid transition from peace to war.

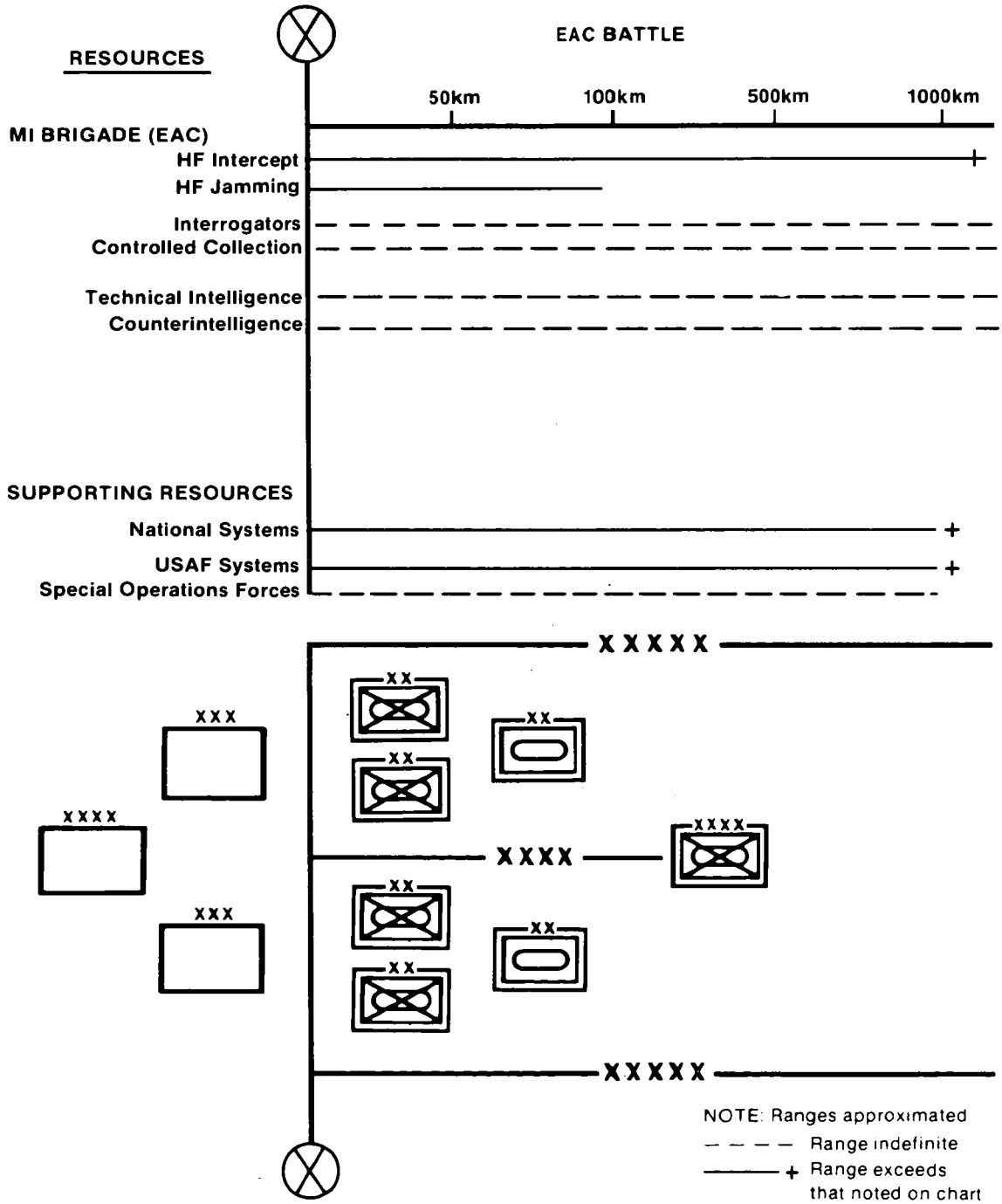
An MI brigade or similar unit provides IEW support to EAC. These MI commands are regionally and functionally tailored to provide multidisciplined IEW support to each theater or contingency force. These units are tailored to fit the mission. They may be an MI brigade as in Korea, an MI brigade as is being formed in Europe, or an MI detachment for some contingencies. Other contingencies may have war plans calling for an EAC MI unit in a reinforcing role to augment a corps MI brigade.

Some Army IEW units will operate at EAC because of decisions at the Joint Chiefs of Staff and Headquarters, Department of the Army levels; because an Army component commander wants them; or because a JTF commander requests them. Still others may be established because the DOD and national intelligence agencies assign missions to the Army. The IEW organizational structure must be sufficiently flexible to accommodate changes in war plans and missions assigned to the IEW command and adjustments in US and allied forces involved.

The design and structure of IEW organizations also require coordination with the other US military service departments and intelligence agencies. In some areas, one service may perform an IEW mission for all. In other areas, the collection responsibilities, CI mission, communications data links, analytic support, and product reporting must be clearly understood in order to structure the Army IEW force.

The diverse nature of EAC organizations, missions, and C^2 relationships create differences in assigned and supporting IEW resources. The resources that would normally be assigned to, and in support of, an EAC command are illustrated as follows.

ECHELONS ABOVE CORPS RESOURCES



Subordinate units and elements of the IEW command at EAC could be placed in support of the corps and other US units and, in some cases, allied and combined commands.

The support relationships in peacetime parallel as closely as possible those support relationships needed in war. This is done in accordance with the reality of the situation, in coordination with the commands involved, and includes direction from the national intelligence agencies. Organizational structures, operating arrangements, and interfaces between the IEW elements and supported commands are such that little change need occur in a transition from peace to war.

The following illustration identifies echelons of command, their fusion centers, and organic IEW resources. Interfaces are shown by arrows between centers in the second column. The allocated support column lists those resources provided as support from the next higher echelon. For instance, the corps line shows CI, TI, and interrogation resources organic to EAC but normally assigned to support corps IEW operations. The last column on the right lists those supporting organizations or echelons from which each echelon in the left column requests support.

IEW SYSTEM

ECHELON	PRODUCERS	ORGANIC RESOURCES	ALLOCATED SUPPORT	REQUESTS SPT FROM
EAC	EACIC	MI Bde (EAC) Intgs S&T Intel HUMINT CI SIGINT HF ECM		USAF/USN/USMC National Allies
CORPS	CTOC SPT ELM	MI Bde Intg CI Spt Voice Coll (VHF) Aerial Noncom Intcp Aerial Comm Intcp VHF ECM (Grd) Noncom Intcp (Grd) SLAR, Photo IA Long-Range Survl	CI Spt Tech Intel Intgs	EAC USAF/USN/USMC National Allies
DIV[1] (HEAVY)	DTOC SPT ELM	MI Bn GSR Aerial Comm Intcp/DF/ECM (OPCON) CI Spt Voice Coll (VHF/HF/ECM) HF/VHF ECM Noncom Intcp/DF Intgs Long-Range Survl	Voice Coll (VHF) VHF ECM (Grd) Noncom Intcp (Grd) INT CI Spt	CORPS USAF
BDE	S2/BICC	No Resources[2]	IEW Spt Elm[3] Survl Sqd IEW Co Tm C&J Plt CI Spt[4] Intg[4]	Div
BN	S2/BICC	Scout Plt Troops Patrols	GSR Tms	BDE

NOTES:

1 ACR/separate brigade organic MI company provides support similar to divisional MI battalion adjusted to scale based on the mission.

2 Some resources are further allocated to the battalion.

3 IEW support element provides interface between MI assets and brigade S2/S3.

4 When corps augmentation is available.

DEPARTMENTAL

Numerous Army organizations at the departmental level perform intelligence missions or provide support to the Army's tactical IEW operations. The principal staff elements at this level are the Assistant Chief of Staff for Intelligence (ACSI) and the Deputy Chief of Staff for Operations and Plans (DCSOPS). The Commander, Intelligence and Security Command (INSCOM), is the primary executor at departmental level.

The ACSI is responsible for the direction, coordination, and development of policy for Army intelligence operations. The office of the ACSI is the policy point of contact for intelligence matters with national level agencies as well as coordination with allied and foreign countries. It is the focal point for SIGINT operations within the Army. The DCSOPS is the functional program manager for tactical intelligence and related activities.

The chart which follows provides an overview of the intelligence organizations at departmental level.

DEPARTMENTAL RESOURCES		
Organization/ Activity	Assigned To	Function
Intelligence and Threat Analysis Center	Army Intelligence Agency	General Intelligence Production and Threat Analysis
Missile and Space Intelligence Center	Army Intelligence Agency	Scientific and Technical Intelligence Production
Foreign Science and Technology Center	Army Intelligence Agency	Scientific and Technical Intelligence Production
Armed Forced Medical Intelligence Center	Surgeon General and ACSI	Specialized Scientific and Technical Intelligence
US Army Intelligence Center and School	TRADOC	Doctrinal and Combat Developments and Training
US Army Intelligence and Security Board	USAICS, TRADOC	Test and Evaluation on Developmental SIGINT and EW Systems

NATIONAL

The national intelligence structure orients on satisfying strategic intelligence requirements in support of national objectives. Still, much of the strategic intelligence collected and produced at this level is of value to tactical levels and is disseminated for use. The actual structure includes all previous resources described as well as those agencies working at the national level and outside DOD.

CHAPTER 3

Situation and Target Development

Situation and target development are the processes that provide commanders the intelligence and targeting data they need to plan and fight the air-land battle. Both processes, conducted simultaneously, incorporate IPB and the intelligence cycle functions. Both are continuous and are performed by commanders and intelligence staffs at all echelons. Begun in peacetime, they become the essence of intelligence production during hostilities.

Situation development enables commanders to see and understand the battlefield in sufficient time and detail to employ their forces and weapons systems effectively. In situation development, the G2 or S2 uses IPB to produce a description of enemy force disposition on the battlefield in terms of location, size, type, direction and rate of movement, and activity. This portrayal is based on an analysis of intelligence holdings which are continuously updated through the collection and processing of information. Situation development consists of—

- ☐ Directing.
- ☐ Collecting.
- ☐ Processing.
- ☐ Disseminating.

Target development is the process of providing timely and accurate locations of enemy movers, emitters, shooters, and sitters that may impact on current and future operations. Effective target development is based on situation development and is accomplished throughout the commander's area of operations and interest. It provides commanders the targeting data they need to effectively attack targets with fire, maneuver, or EW means.

Situation and target development represent the essence, or final goal, of the intelligence production process at the tactical level. Both are dependent on the collecting, processing, and disseminating of information. This chapter describes how the collection management, processing, and dissemination functions are performed at ECB to support situation and target development. It focuses on collection management procedures; the recording, evaluation, and interpretation of information; and dissemination requirements and means.

IPB, in addition to being an information processing function, provides a basis for accomplishing situation and target development. IPB orients the mission planning, collection, processing, and dissemination efforts of situation and target development. Because of its important role, IPB is described first so that the other functions in this chapter can be better understood.

Mission planning is the initial step in preparing for war or for future operations during war. Mission planning guides the IPB process by focusing on unit contingency areas. It draws together, in priority, the information needed to build the IPB data base.

Upon receipt of a mission, commanders analyze it to determine its key elements. They complete the analysis based on the analysis of the battlefield area presented by the G2 and available information provided by other staff members. After completing mission analysis, commanders restate the mission and issue planning guidance. Planning guidance results in the preparation of staff estimates. The intelligence estimates along with other staff estimates are presented to commanders for use in determining what actions must be taken to accomplish the mission. Using these estimates commanders decide on a course of action and announce their concept of the operation.

The commander's guidance and concept of the operation are the basis for action by

his staff. From these and individual analyses of the mission, team members determine what IEW requirements must be satisfied to prepare and execute the mission and build the IPB data base.

The staff mission analysis is the first step in determining planning requirements. Each staff member analyzes the commander's restated mission to determine the specific tasks to be performed. They consider the effects of individual requirements on the planning of their own and other staff sections and subordinate units.

Once the staff has determined its planning requirements, a great deal of information will be required for the IPB effort and the analysis of the battlefield area. In most cases, the G2 will be responsible for acquiring all the needed information. Each staff member identifies individual requirements of the command and identifies the probable sources of the data.

The G2 staff focuses planning requirements on answering questions about the enemy, weather, and terrain. Generally, the G2 staff plans for—

- ☐ Acquisition of current intelligence for initial command and staff planning.
- ☐ Dissemination of intelligence.
- ☐ Acquisition of intelligence during movement.
- ☐ Collection, processing, and dissemination of information after deployment.
- ☐ CI support before, during, and after the operation.

The G2 needs information to satisfy individual planning needs and provide other staff elements (G3, G4, engineer, aviation, and so forth) and subordinate units the information they need. Information needed includes—

- ☐ Composition, disposition, equipment, and effectiveness of enemy forces in the mission area.
- ☐ Terrain, trafficability, ground and air avenues of approach, barriers, obstacles, line of sight (LOS), and climatic conditions.

The G3's IEW planning requirements are in the areas of targeting, EW, deception, and OPSEC to support maneuver, C^3CM, and rear operations. Generally the G3 plan for—

- ☐ Integration of jamming and deception with fire and maneuver.
- ☐ Protection of the combat force during the planning period, movement, and after arrival in the area of operations.

In addition to information to support fire and maneuver, the G3 needs information to support ECM, deception, and OPSEC planning. To support these functions, the G2 provides the commander and G3 information about the—

- ☐ Enemy situation.
- ☐ Weather conditions.
- ☐ Terrain.
- ☐ Long-range operational requirements.
- ☐ IEW needs and special requirements in the area of interest.
- ☐ Enemy EOB.
- ☐ Enemy EW capability.
- ☐ Enemy intelligence capability.
- ☐ Reliability of local nationals.
- ☐ Enemy vulnerability to deception.

Most of the information needs of the command are obtained from the G2's current intelligence holdings and from supporting agencies.

Procedures for intelligence acquisition are outlined in the ACSI, DA, "Army Plan for Crisis Intelligence Support to CONUS Army Units." (This plan applies only to time-critical crisis situations short of general war. It is available from major Army commands (MACOMs) or the originator.)

The Defense Intelligence Estimate (DIE) and Special Defense Intelligence Estimate (SDIE) prepared by the Defense Intelligence Agency (DIA) and the National Intelligence Estimate (NIE) and Special NIE prepared by the Central Intelligence Agency (CIA) can supply some of the initial intelligence required by the commander and the IEW staff.

Units tasked by the Joint Chiefs of Staff may submit requests directly to DIA in time-critical crisis situations. Any unit requesting DIA or other national assistance directly must keep the chain of command informed, including the appropriate unified command. The Intelligence and Threat Analysis Center (ITAC) of the Army intelligence Agency provides additional intelligence as well as support for routine or less time-critical requirements. Requests are forwarded by message. In most cases, higher headquarters will authorize direct coordination with other intelligence agencies.

Additionally, information may be obtained from—

- ☐ Gazetteers, catalogs, and maps from the Defense Mapping Agency (DMA), US Coast and Geodetic Survey, National Aeronautics and Space Administration (NASA), and the CIA.
- ☐ Country studies available through DA publication channels (DA Pam 550-Series), Superintendent of Documents; US Government Printing Office; State Department; CIA; DIA; and United States Information Agency (USIA).
- ☐ Threat analysis, S&T intelligence, OB, and EOB data available from ITAC, Foreign Science and Technology Center (FSTC) of the Army Intelligence Agency, US State Department, NSA, CIA, DIA, Joint EW Center, the USAF Electronic Security Command, Naval Intelligence, Air Force Intelligence, USAREUR, and EUCOM.
- ☐ Imagery and analysis of imagery available from the National Photo Interpretation Center (NPIC).

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

IPB is a systematic and continuous process of analyzing the enemy, weather, and terrain in a specific geographic area. This approach integrates enemy doctrine with the weather and terrain, the mission, and the specific battlefield environment. IPB helps to systematically determine and evaluate enemy capabilities and vulnerabilities.

The IPB process is continuous. It concentrates on building the IPB data base prior to hostilities and outlines its applicability in support of tactical operations. This results in an intelligence estimate and analysis of the battlefield area which shows probable enemy courses of action and intentions. Mission planning sets the IPB process in motion.

Graphics are basic to IPB analysis. Most intelligence can be communicated with pictures. Annotated military maps, multilayered overlays, gridded photomaps, microfilm, and large-scale map substitutes, all capable of computer-assisted cathode ray tube display, are used in the IPB process. These graphics become the basis for intelligence and operational planning. The analysis of the battlefield area and the intelligence estimate are not replaced by graphics, but are merely converted to them where possible. Currency is maintained through graphic renewal or update.

IPB provides a basis for collection management planning before the battle and guides the effective employment of collection resources during the battle. The graphic data bases developed and maintained through IPB, coupled with conventional data bases, provide a foundation for situation and target development. They provide a means for projecting significant battlefield events and enemy activities and for predicting enemy intentions. By comparing them with actual events and activities as they occur, the G2 can provide the commander with timely, complete, and accurate intelligence.

ORGANIZATION

IPB requires the dedicated efforts of the entire IEW staff as well as the support of numerous other elements of the command. IPB is routinely performed at all echelons, battalion through corps, in combat, combat support, and CSS units. Detailed IPB products (overlays and doctrinal templates) are prepared at corps and division, which provide needed products to brigades and battalions to assist their IPB by compensating for their lack of time and personnel resources. Below brigade, the IPB process is less formal, producing detailed products only when time and resources permit.

The G2 serves as the coordinator of the IPB effort. He is assisted by the integrated efforts of OB technicians and intelligence analysts of the ASPS, the engineer detachment (terrain team), and the Air Force weather team. The G2 ensures that IPB focuses on the intelligence needs of the command. The ASPS assembles the threat data base, converts it to graphics where possible, and integrates it with the weather and terrain information. It develops the IPB products that are used to support combat operations. The engineer detachment analyzes terrain and weather data to determine their integrated impact on friendly and enemy tactical and logistical operations. The engineer detachment, supported by its EAC engineer topographic battalion, provides special terrain and map products. The weather team provides climate and weather data to support the IPB effort.

PROCESS

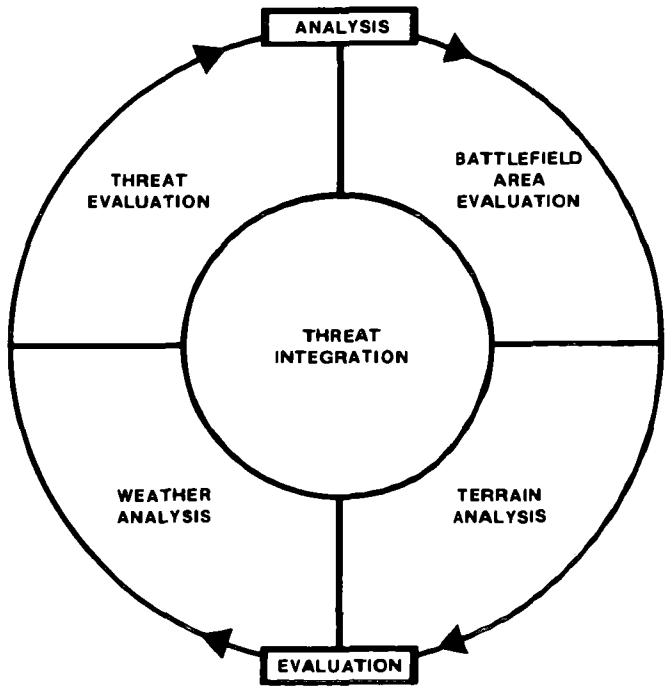
IPB orients on the AO, the area of interest, and the enemy forces that are expected to be operating in those areas. The following illustration shows the five-function cycle IPB process: battlefield area evaluation, terrain analysis, weather analysis, threat evaluation, and threat integration.

The illustration on page 3-5 outlines the IPB roles and responsibilities and highlights the IPB function where each is most important.

Templates are vital to the IPB process. A template, normally drawn to scale, is a graphic illustration of enemy force structure, deployment, or capabilities. It provides a means for seeing the battlefield and a sound basis for command judgments and decisions affecting resource allocation. It is used as a comparative data base to integrate what we know about the enemy with specific weather and terrain information.

Templates enable us to visualize enemy capabilities, predict likely courses of action

IPB PROCESS



IPB ROLES AND RESPONSIBILITIES		
ELEMENTS	ROLE/RESPONSIBILITY	IPB FUNCTION (see text)
Force Cdr	Uses decision support templating.	5
G2	Overall coordinating	All
G3	Assists in event and decision support templating. Formulates requirements.	5
ASPS	Threat analysis. Integrates threat, weather, and terrain information.	1, 4, and 5
Engineer Detachment (Terrain)	Terrain and weather analysis.	2 and 3
Weather Tm	Provides weather data and associated technical analysis support.	3

before the battle, and confirm or refute them during combat. Templates also provide a means for continuous identification and assessment of enemy capabilities and vulnerabilities. Information graphically displayed on templates can be added to, changed, or deleted as the situation changes.

The following chart describes the four principal types of templates developed during the IPB process and explains how and when each should be used.

Function 1

The first function of the IPB process is battlefield area evaluation. When the areas of operations and interest are applied to the battlefield, the analyst's attention is focused on a specific geographical area for enemy, terrain, and weather effects analysis.

The limits of the command's area of operations (fire, EW, and maneuver) are prescribed by higher headquarters. There is no limit to a unit's area of interest; it is recommended by the G2 or S2, based on METT-T, and approved by the commander. The dimensions of the areas of operations and interest are in terms of width, depth, airspace, and time.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD TEMPLATES			
TEMPLATE	DESCRIPTION	PURPOSE	WHEN PREPARED
Doctrinal	Enemy doctrinal deployment for various types of operations without constraints imposed by weather and terrain. Composition, formation, frontages, depths, equipment numbers and ratios, and high value targets are types of information displayed.	Provides the basis for integrating enemy doctrine with terrain and weather doctrine. In processing, information used to establish probable locations of unlocated units.	Threat Evaluation
Situation	Depicts how the enemy might deploy and operate within the constraints imposed by the weather, terrain, and current strength.	Used to identify critical enemy activities and locations. Provides a basis for situation and target development and HVT analysis.	Threat Integration
Event	Depicts locations where critical events and activities are expected to occur and where HVT will appear.	Used to predict time-related events within critical areas. Provides a basis for collection operations, predicting and confirming enemy intentions, and locating HVT.	Threat Integration
Decision Support	Depicts decision points and target areas of interest keyed to significant events and activities. The intelligence estimate in graphic form.	Graphically establishes a decision to time/space relationship. Used to prepare commanders to make tactical decisions relative to battlefield events. Assist the commander/staff in synchronizing the battle.	Threat Integration

In addition to METT-T and the commander's concept of the operation, the G2 or S2 must consider several other factors when recommending the unit's area of interest. Foremost is the security of the command. The area of interest must extend (in as irregular a shape and as far as needed) in all directions to safeguard the command from surprise. The area of interest must also be deep enough to support planning for future operations. But the limits of the area of interest are forwarded to the next higher echelon to guide their support of unit collection requirements. Therefore, the area of interest must not be so large that incoming information from higher echelons overwhelms the unit's analytic and processing capabilities.

Function 2

The second function of the IPB process is terrain analysis. This function is focused on the military aspects of the terrain and their effects on friendly and enemy capabilities to move, shoot, and communicate. This includes the following five factors (short title: OCOKA):

- ☐ Observation and fields of fire.
- ☐ Concealment and cover.
- ☐ Obstacles.
- ☐ Key terrain.
- ☐ Avenues of approach and mobility corridors.

Observation and Fields of Fire. Observation relates to the impact terrain has on the capability of battlefield systems. In the IPB context, it refers primarily to visual and electronic LOS determined through LOS analysis.

Many battlefield systems require LOS to function effectively. These systems include radios, radars, ESM systems and direction finders, jammers, direct fire weapons, and human vision.

Concealment and Cover. Concealment is protection from observation. Cover is protection from the effects of fire. Concealment is vital to OPSEC and deception. Concealment and cover offered by the terrain to both friendly and enemy forces is determined through IPB.

Obstacles. Obstacles are natural and artificial terrain features that stop, canalize, impede, or divert military movement. Their direct influence on mobility makes them one of the most important considerations in terrain analysis.

Key Terrain. Key terrain is any feature or area of which, the seizure, retention, or control will affort a marked advantage in the conduct of operations to either combatant. The determination of key terrain is dependent on the echelon of the command, the mission, the enemy and the situation.

The commander may designate certain key terrain as decisive terrain if it will have an extraordinary impact on the mission. To designate terrain as decisive is to recognize that the mission depends on seizing or retaining it.

Avenues of Approach. Avenues of approach are air or ground routes by which a force may reach an objective or key terrain. They are evaluated in terms of their—

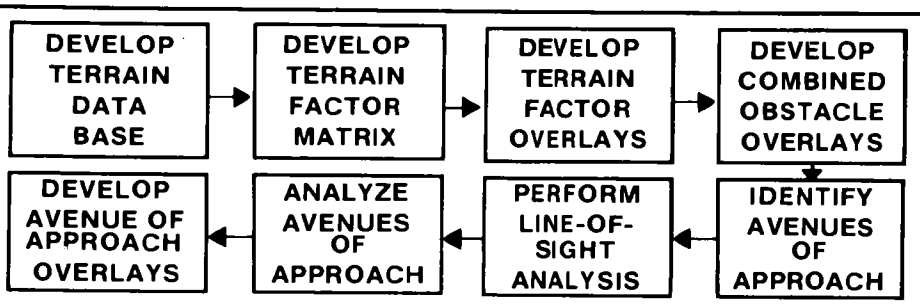
- ☐ Potential to support maneuver.
- ☐ Access to the terrain and adjacent avenues.
- ☐ Degree of canalization.
- ☐ Concealment and cover.
- ☐ Observation and fields of fire.
- ☐ Obstacles.

The terrain analysis process emphasizes the use of graphics to portray the effects of trafficability and intervisibility on operations. A terrain factor matrix and a series of overlays are prepared to develop a terrain graphic data base to facilitate threat integration (function 5).

Several steps are followed to organize and refine the information needed to accurately analyze a specific piece of terrain. The following illustration depicts those steps.

The terrain factor matrix guides the selection of terrain and weather factor overlays needed to analyze the terrain. Engineer terrain analysis begins with a detailed review of the terrain data base to identify information gaps. The illustration on page 3-8 is an example of a terrain factor matrix.

TERRAIN ANALYSIS PROCESS



TERRAIN FACTOR MATRIX

FACTORS

FUNCTIONS	Surface Configuration (Slope)	Surface Materials (Soils)	Vegetation	Weather Effects on Terrain	Transportation	Obstacle (Linear)	Built-up Areas	Surface Drainage (Hydrology)
Observation and FofF	X		X	X	X		X	
Concealment and Cover	X		X		X		X	
Assembly Areas	X	X	X		X		X	
Key Terrain	X			X	X		X	
Ground Aves of Approach	X	X	X	X	X	X	X	X
Air Aves of Approach	X		X	X	X	X	X	
Weapon Sites	X	X	X	X	X	X	X	X
DZ and LZ	X	X	X	X	X	X	X	X
Maneuver	X	X	X	X	X	X	X	X
LOC and MSR				X	X	X	X	
Barriers and Fortifications	X	X	X	X	X	X	X	X
LOS	X		X	X	X	X	X	
Comm Sites	X	X	X	X	X	X	X	
EW Sites	X	X	X	X	X	X		

Terrain factor overlays graphically portray the military aspects of terrain (types and spacing of vegetation, soil, and climate conditions and variations) in the AO.

The final step of the terrain analysis process selects the avenue of approach that supports friendly and enemy capabilities to move, shoot, and communicate. FM 100-5 further describes terrain analysis and its importance to tactical operations.

Function 3

Weather has a significant impact on both friendly and enemy capabilities. Analyzing the weather in detail to determine how it affects friendly and enemy capabilities to

WEATHER FACTOR ANALYSIS MATRIX

INTELLIGENCE USES/ APPLICATIONS	Temperature[1]	Humidity[1]	Intervisibility	Surface Winds	Precipitation	Snow/Ice Cover	Winds Aloft	Cloud Data	Light Data	Severe Weather	Fog
Observation and FofF			X	X	X	X		X	X	X	X
Artillery Emplacements	X	X		X	X		X			X	
Concealment			X	X	X	X		X	X	X	X
Camouflage	X	X	X	X	X	X		X		X	X
Ground Avenues of Approach	X		X		X	X				X	X
Air Avenues of Approach	X	X	X	X	X	X	X	X	X	X	X
Cross-Country Movement	X		X	X	X	X			X	X	
Fording Sites	X		X	X	X	X			X	X	X
Air Drop Zones	X		X	X	X	X	X	X	X	X	X
Helicopter and STOL/VTOL LZ/PZ	X	X	X	X	X	X	X	X	X	X	X
LOCs and MSRs	X		X		X	X		X	X		
NBC Operations	X	X			X	X	X	X		X	X
Line-of-Sight (Radio/Radar)					X	X				X	
REMS Emplacement	X			X	X	X				X	
Infiltration Routes			X		X	X			X	X	X

1 Density altitude quality affects helicopter lift capacity.

move, shoot, and communicate is critical to this function of IPB. Because the weather has a tremendous effect on terrain, terrain and weather analysis are inseparable factors of intelligence.

Weather and engineer terrain teams work together during much of the analysis process. The weather team analyzes climatic data to determine the characteristics of weather in the battlefield area. The terrain team analyzes the effects of weather on tactical operations and integrates climatic and current weather data with terrain analysis. This information is integrated into a three-step operation known as the weather analysis process. This process incorporates developing a weather data base, a weather factor analysis matrix, and weather factor overlays to determine the impact of weather on terrain and operations.

During peacetime, historic weather conditions for at least five years past are used to determine significant weather parameters in the area of operations. The weather team focuses on specific periods within each season that may deviate from the seasonal norm. The weather data base is continually updated and is used as the foundation for analyzing the effects of weather on tactical operations.

The weather factor analysis matrix helps to determine what weather effects overlays will be required. It identifies the weather factors that are militarily significant and correlates their effects with specific intelligence uses and tactical applications. The previous illustration is an example of a weather factor analysis matrix. Detailed data on the effects of weather on friendly and enemy forces can be found in FM 34-81.

As in terrain analysis, maximum use of graphics is instrumental in analyzing the effects of weather on combat operations. Through weather effects overlays, weather data is converted into graphic displays.

Various weather effects will have significant impact on tactical operations. Cloud cover at low levels will have a significant impact on low level attack helicopters, CAS, aerial visual observation, and some aerial surveillance systems.

The effects of precipitation can be graphically illustrated as follows.

The illustration shows riverbanks and swamps that have swollen, rendering fording and hasty river crossings more difficult.

A combined obstacle overlay combines all terrain- and weather-induced obstacles resulting from this analysis. It focuses on significant terrain areas. Next, avenues of approach and mobility corridors (MCs) are identified. Avenues of approach are identified for friendly or enemy forces at the same echelon and one below, and MC for forces two echelons below. Once the most viable avenues of approach and MCs have been selected, overlays are prepared depicting each. Analysis enables the development of LOS for weapons, communications, target acquisition, intelligence collection, and ECM systems for each option.

Function 4

The fourth function of the IPB process is threat evaluation. It consists of a detailed study of enemy forces, their composition and organization, tactical doctrine, weapons and equipment, and supporting battlefield functional systems. The thrust of this function is to determine enemy capabilities and how they operate as prescribed by their doctrine and training.

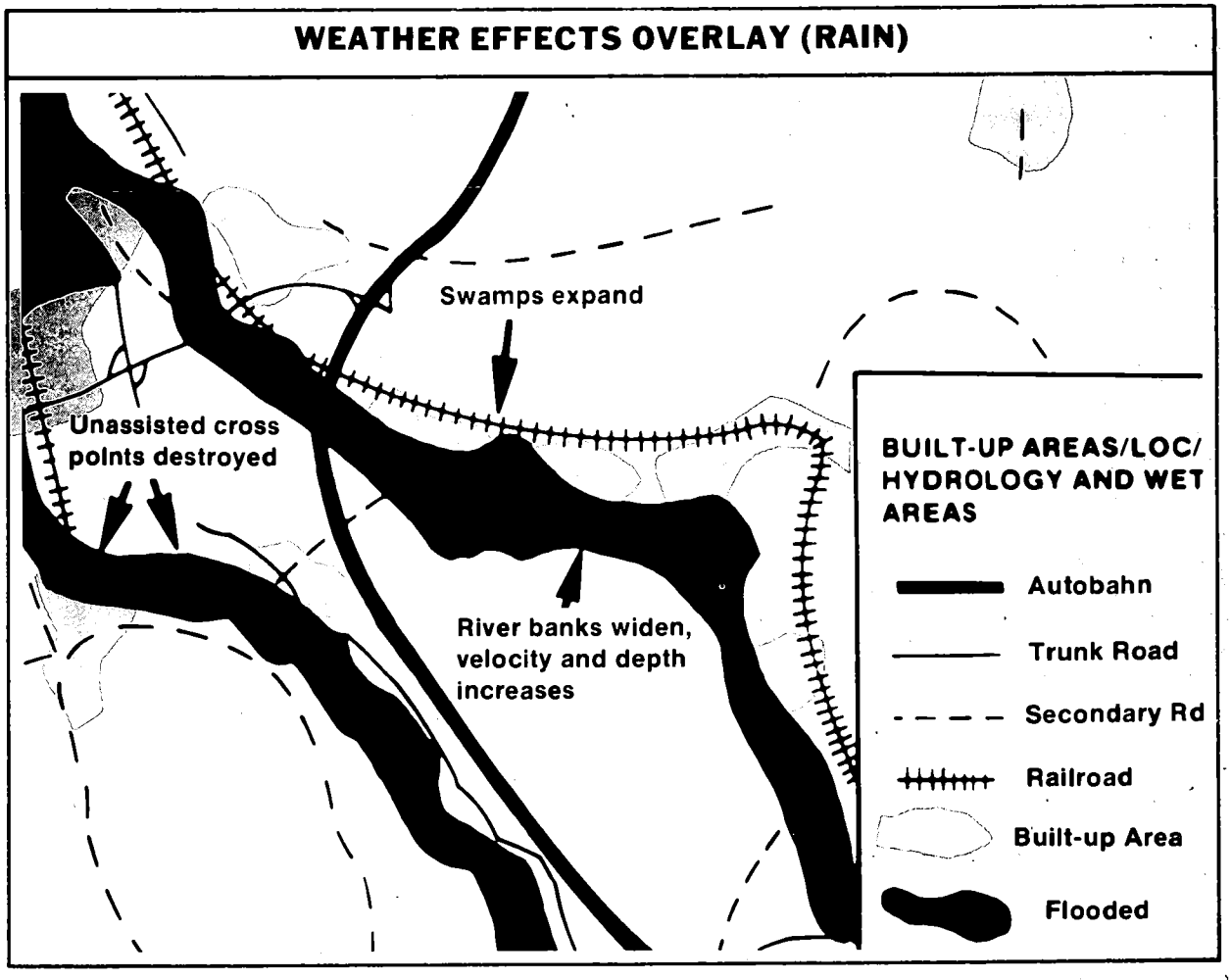
Threat evaluation also includes an evaluation of HVTs and doctrinal rates of movement. HVTs and movement rates are reevaluated during threat integration (function 5) within the constraints imposed by the terrain and weather. Threat evaluation is a continuing process as new capabilities to wage war develop, and as doctrine changes. Threat evaluation follows a multistep process.

Development of a detailed threat OB data base by the ASPS is vital to threat evaluation. A current, accurate, and comprehensive data base on potential enemy forces facilitates a thorough evaluation of their doctrine and capabilities. To develop the threat data base, a review of the mission and area of interest is required. Through this review, identification and isolation of threat forces significant to the mission are accomplished. As information about the

enemy is assembled, gaps are identified and information requirements fed to the CM&D section.

When the threat data base has been developed and evaluated, the G2 and the ASPS must determine what doctrinal templates are required. Determining which enemy echelons should be the focal point of attention is the first step. Generally, the "one up and two down" formula is used so that attention is concentrated on those enemy echelons that pose the greatest threat.

Requirements for doctrinal templates of battlefield functional systems are also identified. Those battlefield functional systems which tell the most about enemy operations are templated. This matrix allows rapid analysis of the relationship between battlefield systems and the operations supported by those systems. It helps the analyst conduct TVA and determine additional needs and requirements.



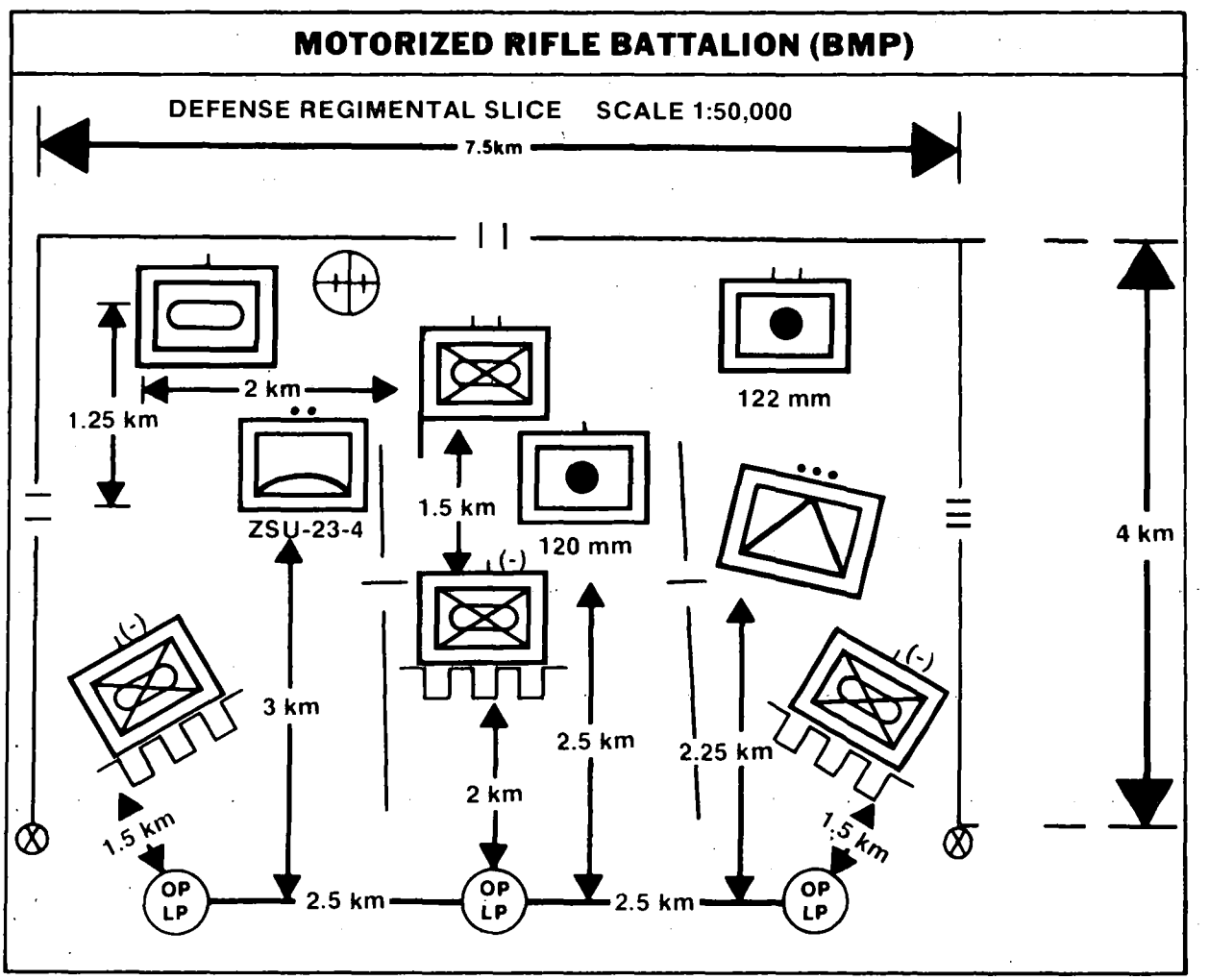
DOCTRINAL TEMPLATE SYSTEMS MATRIX							
TYPES OF BATTLEFIELD SYSTEMS / TYPES OF COMBAT ACTIONS	MARCH	MEETING ENGAGEMENT	RIVER CROSSING	ATTACK AGAINST A DEFENDING ENEMY	PURSUIT	HASTY DEFENSE	PREPARED DEFENSE
TACTICAL ROCKETS AND ARTILLERY	X	X	X	X	X	X	X
AIR DEFENSE	X	X	X	X		X	X
COMMUNICATIONS	X	X	X	X			X
REC		X	X	X	X	X	X
ATGM				X	X	X	X
RECONNAISSANCE	X		X		X	X	X
REAR SERVICES			X	X	X		X
C^2 OF MRD	X	X	X	X	X	X	X
C^2 OF MRR	X	X	X	X	X	X	X
ENGINEERS	X		X	X	X		X

Doctrinal templates convert enemy OB factors into graphic portrayals. They are models of how the enemy might look according to doctrine and training if not constrained by the weather and terrain. They portray various echelons and types of units for various capabilities and schemes of maneuver. They also graphically portray the composition and disposition, frontages and depths, and spacing and signatures of

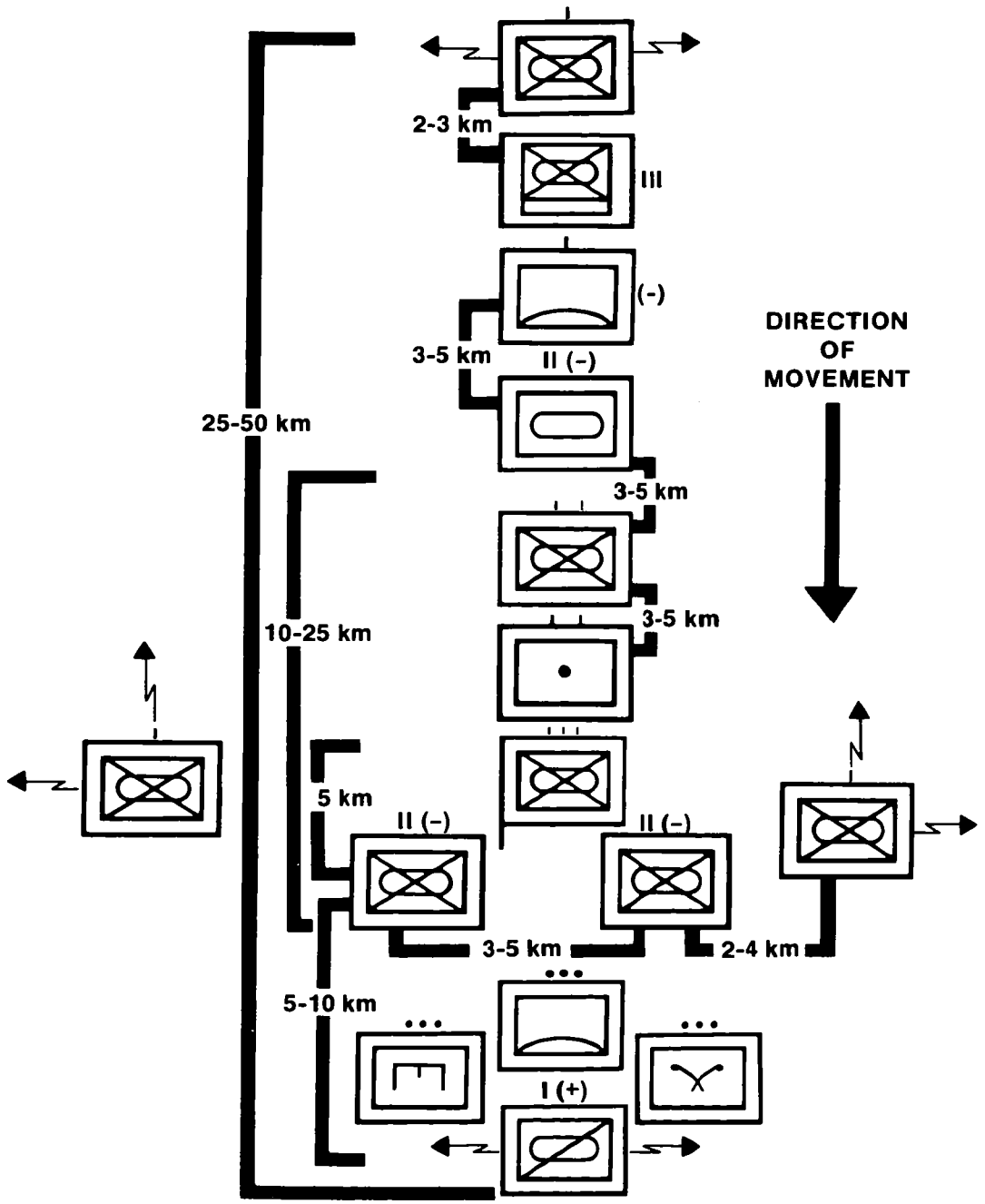
these echelons and units. The following illustrations provide examples of doctrinal templates.

The final step in determining doctrinal template needs is to compare current requirements to previously prepared templates. If additional templates are needed, the analyst must request or prepare new ones.

Doctrinal templates may include a portrayal of higher echelon supporting elements or elements normally deployed with the unit being templated. They may be further refined into doctrinal template subsets. These subsets might include battlefield functional systems or weapons and equipment deployments. Such templates, especially those depicting weapons and equipment deployments, are very useful in identifying types of enemy units and specific formations. Subsets may be equally useful in determining enemy intentions.



MRR PREBATTLE FORMATION (REVERSE WEDGE)



Function 5

The nucleus of the IPB process is the integration of enemy doctrine with weather and terrain data. The objective of threat integration is to determine how the enemy will fight as influenced by weather and terrain. Threat integration, a sequential process, is accomplished through the development of situation, event, and decision support templates.

Situation Template. A situation template depicts enemy dispositions for a specific instant in time. Thus, several situation templates or situation "snapshots" may be created to show how the enemy may change his disposition during the conduct of an operation.

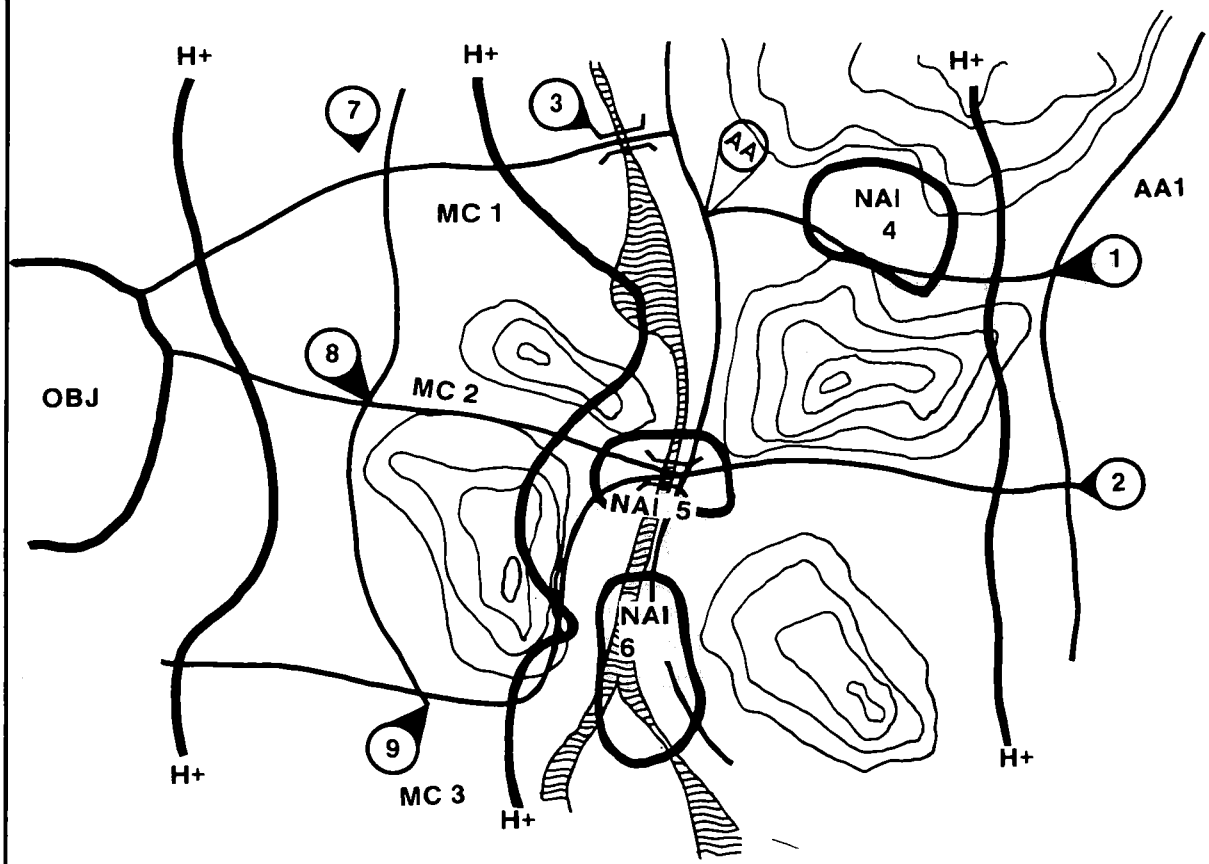
Event Template. Once the analyst has hypothesized the probable enemy course of action, he creates an event template to test his hypothesis. The event template provides the information needed to project what events will most likely have to occur relative to enemy courses of action. As an enemy force moves along an MC, it will be required to do certain things at certain times and places which are dictated by terrain, weather, and tactics. Based on this, the analyst selects named areas of interest (NAIs) where he expects to see certain activities or events which have tactical significance. The analyst projects a sequence and timing of events based on an analysis of the relationship of NAIs to one another and to specific available courses of actions. Activity, or the lack thereof, confirms or denies the enemy course of action. In the following illustration, which is an example of an event template, NAIs 1 through 9 are areas where particular types of activity would provide indications of intent. The event template is particularly useful to guide intelligence collection management.

NAIs, are points or areas along a particular avenue of approach or MC where activity, or lack of it, will help to confirm or deny a particular enemy course of action. NAIs are only plotted on the event template.

Activity in NAI 1 would indicate whether MC alpha or bravo was being adopted as the route of advance. Forward movement of enemy bridging elements as the force approached a destroyed bridge at NAI 5 would be an indication that a river crossing would be attempted rather than a move to NAI 6 where river crossing would be less difficult. Other NAIs in the example represent intermediate points for collection planning purposes or tracking for target development purposes. An example of how one leg of an MC might be represented is shown in the event analysis matrix shown on page 3-17.

The matrix enables the analyst to more precisely correlate what event or activity is expected within the geographical location and at what time the event is expected to take place. The event analysis matrix is normally prepared at divisions and above. This capability, along with doctrinal and situation templates, provides the basis for critical node or HVT analysis. The estimated times between NAIs within an MC are derived by determining the effects of terrain and normal seasonal conditions (derived from earlier functions) on doctrinal rates of advance (opposed or unopposed, as appropriate). The event template and event analysis matrix allow for the initiation of precise collection requirements, maximizing the use of limited collection assets against the vast array of potential targets on the future battlefield. By knowing in advance what the enemy can do and comparing it with what he is doing, the analyst has the basis for predicting what the enemy intends to do next. Such information provides the basis for cuing intelligence collection and constructing decision support templates (DSTs).

EVENT TEMPLATE



H+ - Time Line: Time lines are developed on doctrinal rates of movements as affected by terrain and weather. Time lines are modified based on actual rates of movement.

1 Point NAI

NAI 5 Area NAI

MC 1 Avenues of approach/mobility corridor by priority

EVENT ANALYSIS MATRIX

AVENUE OF APPROACH II

COORDINATES
FM: NB 606330-NB 650333
TO: NB 462181-NB 494132

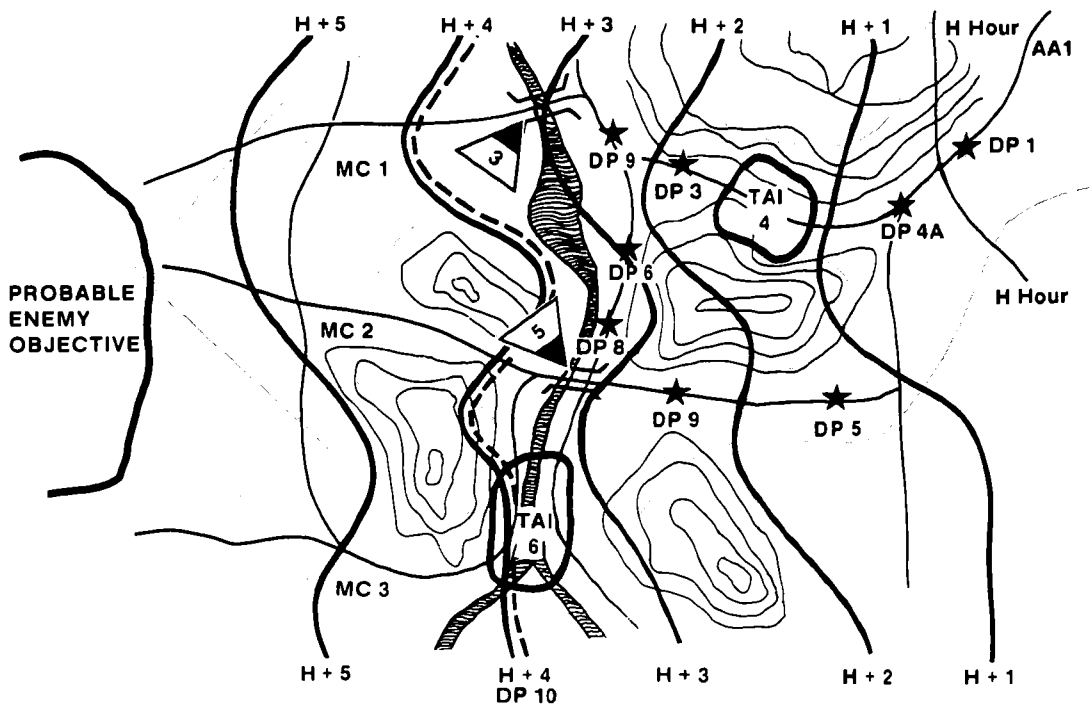
MOBILITY CORRIDOR # 1

FM: NB 670300
TO: NB 468158

NAMED AREA OF INTEREST	DISTANCE	ESTIMATED TIME	EVENT/ACTIVITY	OBSERVED TIME
NAI #1 NB 649288 RD JUNCTION	2.5KM	9 MIN	A. RECON ELM	1500
			B. ADV GUARD	1510
			C.	
NAI #4A NB 647264 CHOKE POINT	6.5KM	25 MIN	A. RECON ELM	1508
			B. ADV GUARD	1520
			C.	
NAI #4 NB 601222 RD JUNCTION	4.0KM	17 MIN	A. RECON ELM	1533
			B. ADV GUARD	1545 EST
			C.	
NAI #3 NB 561220 BRIDGE	8.5KM	30 MIN	A. RECON ELM	1544 EST
			B. ADV GUARD	1556 EST
			C.	
NAI #7 NB 480180 RD JUNCTION			A.	
			B.	
			C.	

Event and decision support templates, the most important products of the IPB process, represent a reduction of all the analysis and template construction tasks that have preceded them into an analysis of the battlefield area and an intelligence estimate. The following illustration shows an example of a DST.

DECISION SUPPORT TEMPLATE



LEGEND

H+ - Time Line: Time lines are developed on doctrinal rates of movements as affected by terrain and weather. Time lines are modified based on actual rates of movement.

★ DP - Decision Points

1 - Point TAI

DP - Decision Line

TAI 2 - Area TAI

MC 1 - Avenue of approach mobility corridor by priority

Decision Support Template. The ultimate objective of threat integration is to provide options for the commander to defeat the enemy. The DST is developed specifically to aid the commander in decision making. The DST does not dictate decisions to the commander, but indicates points where tactical decisions are required.

The DST relates events, activities, and targets of the event template to the commander's decision requirements. It is basically a graphic intelligence estimate and operations plan combined. The commander, G2, G3, FSE, and EWS develop the DST by overlaying the event template, war gaming enemy courses of action, and then placing decision points (DPs) and TAIs to cue friendly courses of action. DPs are placed on the template at those points where the friendly commander must decide which planned courses of action to employ either to effect an enemy course of action or to change a friendly course of action.

A TAI is an area or point, usually along an MC, or is an engagement area where interdiction of enemy forces by maneuver, fires, and jamming will eliminate or reduce a particular enemy capability. It can also cause the enemy to abandon a particular course of action, or require the use of unusual support to continue operations. (In the latter case, the TAI is chosen based on terrain to inhibit or deny movement.) TAIs are developed by the G3 based on the commander's intentions and in coordination with the G2, FSE, and EWS.

A decision point is a point or line usually along an MC where presence of an enemy or friendly unit cues the commander to make a decision. DPs may be independent of, or associated with, a TAI. In the latter case, the DP is that point where the commander must decide whether or not to cue an engagement option in order to have the desired effect on the enemy at the associated TAI. DPs, independent of TAIs, are used to cue some other form of action. For example, when the enemy gets to a certain point on the battlefield, the commander may have to decide to displace the TOC or shift unit positions. In another example, when a friendly unit gets to a certain point on the battlefield, the commander may have to decide to move supporting artillery or change an attack option. DPs are developed by the G3 based on friendly actions/rates of movement or in coordination with the G2 based on enemy actions/enemy rates of movement.

A time-phase line (TPL) is drawn across an avenue of approach or MC to illustrate potential enemy advance at his doctrinal rates, as modified by terrain and weather. TPLs project for the commander the point at which the enemy plans to be at any given time. TPLs do not show the effects of friendly action, except insofar as light or heavy opposition is built into enemy doctrinal rates of advance.

DPs shown in the illustration represent areas chosen because of time and distance factors from TAIs. If a decision is not made by the commander before an enemy force reaches or passes a DP, a set of options which had existed may be negated. For example, DP 1 is associated with an option to route the enemy force to MC 1 by blowing the bridge at TAI 5 before the enemy reaches the first road junction. If the force has moved too far toward MC 2 before the bridge is blown, the enemy may decide to use that route anyway and attempt a river crossing operation rather than backtrack to MC 2. Thus, the placement of DP 1 must include enough time for the blown bridge to be reported back to the enemy commander. The decision to blow the bridge at TAI 5, if the option is to delay, will have to be made by the time the enemy reaches DP 5 or there may not be time to destroy the bridge before the enemy crosses.

DPs may also be used to trigger attacks on TAIs by fires, maneuver, and EW, or to trigger friendly maneuver options. For some TAIs, a definite attack option will have been specified. DPs for these TAIs need to be located so that the time needed to report the enemy presence and execute the attack is equal to or less than the time the enemy force will take to move from the DP to the TAI. For other TAIs, a series of options may be available. In that case, several DPs will be designated, reflecting the response times of the different options. Such a series of DPs related to one TAI is called a DP cluster. DP clusters are used to synchronize

several attack options. Regardless of location, DPs and TAIs should be under surveillance. DPs can also be used to support the operational plan by alerting the commander to the satisfaction of predetermined conditions for maneuver options such as exploitation or counterattack. These options will be developed as the commander, G2, and G3 war game the operation before the battle. This will speed the decision making process so the commander can seize the initiative.

Also depicted in the graphic are potential MCs with the indication that MC 1 would best support the main attack. TPLs and key terrain (cross hatched areas) may also be shown as in the example. Other information, such as combat force ratios and a situational depiction of how the enemy might have to deploy within each avenue, is added as required.

In addition to supporting the development of intelligence for the commander, threat integration supports the intelligence collection effort. Situation templates and event analysis matrices are used to establish collection priorities based on those courses of action the enemy is most likely to adopt. Movers and emitters, the primary indicators of events and activities, can be framed in time and location allowing the collection manager to determine the optimum mix of collection resources. Of the many NAIs plotted by the analysts, threat integration guides the collection manager in deciding which NAI to cover at any particular time.

COLLECTION MANAGEMENT

Collection management is performed by the CM&D section supported by the ASPS. It is the timely, efficient process of formulating detailed collection requirements and tasking collection agencies for required information. The overriding purpose of collection management is to use the limited resources available to answer the commander's priority intelligence requirements.

COLLECTION MANAGERS

The G2 or S2 is the principal collection manager, assisted by collection managers in the CM&D section. Collection managers in the CM&D section receive approved PIR and IR from the G2. They place each requirement in priority order, based on G2 guidance, and plan how to satisfy each. Specifically they—

- Assess collection and reporting implications of each new requirement and plan collection operations.
- Develop multidisciplined tasking that exploits the capabilities of intelligence resources, reflects established priorities, and detects enemy deception attempts.
- Identify and task collection units or agencies.
- Maintain a constant awareness of the operational status of collection resources.
- Evaluate requirement satisfaction, provide requester feedback, and adjust collection plans.

Specific collection planning steps and considerations that optimize collection results include—

- Checking with the ASPS first to see if a request for intelligence information (RII) can be answered with data already available.
- Keeping current with the event template and the changing terrain, weather, and enemy situation data available to the ASPS.
- Developing a collection plan that results in the collection and reporting of information in a logical and orderly manner.
- Considering collector status, capabilities, and limitations for each situation.
- Maximizing multi-disciplined operations and emphasizing cuing, expansion, and verification.
- Providing continuity of operations.
- Ensuring that collection units or agencies are given specific orders and requests.
- Asking higher headquarters for information and verification.
- Ensuring that collection requirements are assigned priorities and are current.

- ☐ Ensuring that timely feedback on request status is provided.

Each of these considerations impacts on the collection planning performed at each echelon. The results of the application of these considerations and the functions of the CM&D section is a collection plan.

COLLECTION PLAN

The collection plan is a dynamic tool used to coordinate and integrate the efforts of all collection units and agencies. Since the collection effort involves continuous planning, an entirely new collection plan is seldom prepared except when a unit first enters combat or enters a new operational phase. The collection plan is continually revised as required.

In effect, it is a slate where new entries are written and outdated entries are removed.

Because information requirements are more complex at higher echelons, the collection plan is normally more extensive and formal at these levels. At any level, however, collection planning is essentially a mental process and the collection plan, regardless of the format being used, is merely an aid. It is not a substitute for thinking and is maintained only to the extent that it assists in planning and supervising the collection effort and maintaining continuity between shifts in the TOC.

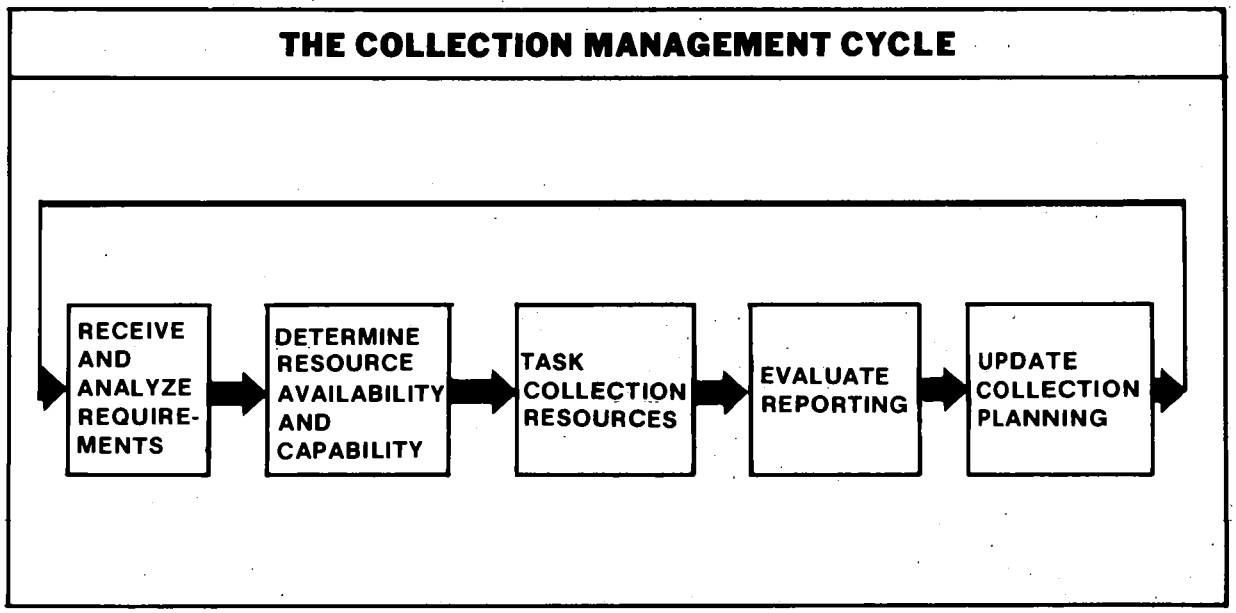
The collection plan is not prepared in any set format. It can be prepared as a simple fragmentary worksheet, a long, detailed plan, or a mental plan. Although a collection manager can formulate a collection plan mentally, the planning of the collection effort is facilitated and is less subject to error when a written plan is used. A written plan, however informal, facilitates continuity of operations and is always recommended.

The type and makeup of the collection plan will depend on the size of the unit, the mission, the situation, and the personalities concerned. Examples of collection plans are found in Appendix H.

COLLECTION MANAGEMENT PROCESS

As shown in the following illustration, collection management is cyclic.

Each collection effort begins by processing IRs. These requirements may take many forms and are generated by many sources: the commander's PIR and IR as identified by the G2, targeting needs of the G3 (FSE and EWS), tasking from higher echelons, and requests for information from



subordinate and adjacent commands. At all echelons, most of these requirements are based on information needs associated with NAI and TAI developed through IPB. Regardless of their origin, the collection manager transforms them into specific collection requirements. This transformation must be performed as quickly as possible while ensuring optimum employment of the limited resources available.

Receive and Analyze Requirements

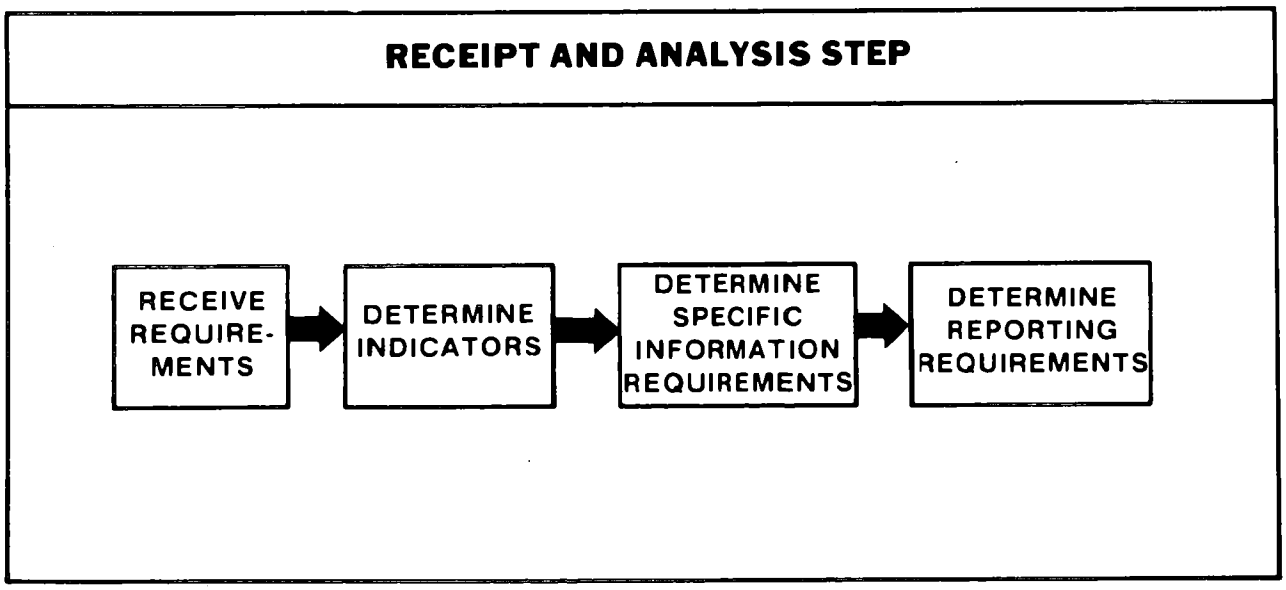
The first step in the collection management process is the receipt and analysis of requirements. An overview of this step is shown in the following illustration.

Receive Requirements. When any requirement is received in the CM&D section it is first logged in the shift journal and identified by assignment of a control number. Requests and tasks from elements outside the headquarters are identified by the control number assigned by the originating headquarters.

Next, the validity of the requirement is determined. A requirement generated outside the command is generally accepted as valid. Requirements from within the command are checked to ensure that each merits commitment of collection and processing resources.

A requirement is then sent to the ASPS where an attempt is made to answer it immediately. This step is important. If the information is readily available the ASPS provides an immediate answer through the CM&D to the requester. This reduces the workload of the ASPS and CM&D section and reduces requirements for collection resources.

The ASPS checks each requirement to see if the information is readily available in its data bases. If the information is not in the data bases, collection subsystems are checked. For example, at the CTOC, the IA section may have acquired imagery that contains the needed information. Other sources such as knowledgeable EPW or the TCAE may be able to answer the requirement if queried within the framework of the requirement. The key is knowing what recently completed collection actions have the potential for answering the requirement. ***Only after available information has been researched should a requirement be validated for new collection action.***



Determine Indicators. A necessary step in directing the collection effort is to determine those enemy activities or characteristics of the battlefield area which answer the information requirement. This procedure is called determination of indicators and is a function of the ASPS assisted by other TOC elements. An indicator is any positive or negative evidence of enemy activity or any characteristic of the battlefield area that points toward enemy capabilities, vulnerabilities, or intentions. The ability to read indicators (including recognition of enemy deception indicators) may contribute to the success of friendly operations, since an analysis of all available indicators will be the basis for recommendations to the commander for a specific course of action.

Indicators form the basis of collection tasks. By knowing those indicators essential to satisfying information requirements, and the most likely methods and places of finding them, the collection manager is able to determine the specific collection tasks to be assigned to available resources. A thorough knowledge of the enemy, the characteristics of the battlefield, and the general capabilities of collection assets is required to develop indicators. Particularly valuable is a detailed knowledge of—

- ☐ The enemy organization, equipment, and doctrine.
- ☐ The personalities of major enemy commanders when possible.
- ☐ The past performance of enemy units.
- ☐ Terrain and weather factors.
- ☐ The event template for current operation.

Indicators have certain characteristics which are considered during the selection process. By considering these characteristics, the best possible indicators can be derived. The determination of indicators is based on those characteristics that reflect—

- ☐ Normal doctrinal activity or disposition.
- ☐ Activity required for a particular course of action.
- ☐ Actions within enemy capabilities and limitations.
- ☐ The characteristics of enemy commanders.
- ☐ Possible or practicable operations.
- ☐ Collection characteristics.
- ☐ Identification of target characteristics.

Event templates are used to determine indicators. They allow the correlation of a particular event or activity with probable enemy courses of action. Additionally, they are used to determine when and where that activity should occur. By determining what events or activities must occur for an enemy to follow a particular course of action, attention is focused on the indicators associated with those events or activities. Event templates help to decide—

- ☐ Where to look.
- ☐ When to look.
- ☐ What to look for.

After determining indicators for each requirement, the ASPS develops specific information requirements for each indicator.

Determine Specific Information Requirements. Indicators and target characteristics are analyzed to determine specific information requirements (SIRs). SIRs are the basic questions that need to be answered to confirm or deny the existence of an indicator.

For example, as an indicator of possible enemy intentions, the location of a particular enemy air defense element is needed. The SIR in this case would be a question asking whether or not there are any ZSU-23-4s at location X. However, such a requirement may be only one part of a broader requirement.

The accurate determination of indicators and SIRs is essential for effective collection management. Knowing where, when, and what to look for helps in selecting what to look with. This in turn maximizes the use of limited collection assets against a vast array of collection targets. After indicators and SIRs have been prepared, the ASPS passes them to the CM&D section for collection action.

After being validated by the ASPS and returned to the CM&D section, new requirements are compared against others in the active collection requirements file. The intent is to identify duplication. If the requirement is a duplicate, the requester's address and other specific needs are noted on the original requirement. When the requirement is answered, each addressee is provided the information needed.

If a requirement is not a duplicate, the copy is filed in the collection file as a control measure and for use in disseminating collected and processed information.

The next step is to evaluate each requirement based on its time sensitivity. The evaluation is made based on the time required to—

- ☐ Process the request.
- ☐ Assign it to a collection unit or agency.
- ☐ Collect and report the information.
- ☐ Process the collected information.
- ☐ Disseminate the resulting intelligence in time to meet the needs of the requester.

Time sensitivity is also considered in light of—

- ☐ The requester's response time to react to the information.
- ☐ Target mobility.

Most time-sensitive requests are annotated with the date-time group (DTG) indicating when the information will no longer be of value.

The next step is to assign a priority to each requirement. The commander's PIRs are always the highest priority collection requirements. IRs, to include requests for information and tasks from higher headquarters, are evaluated based on SOP and G2 guidance. Requests and requirements from outside the headquarters generally carry a priority assigned by the originators. These priorities are evaluated in light of current collection actions and integrated with existing priorities as appropriate. The primary basis for determining the priority of any requirement is its criticality to friendly mission accomplishment and the time the information is needed or will no longer be of value. Priorities must be passed to collection agencies to ensure that they collect what is needed, rather than that which is easy. Requirements are listed on the collection plan by priority, and reporting requirements are determined for each.

Determine Reporting Requirements. Reporting requirements specify when, where, and in what detail information is to be reported. Reporting requirements are developed in terms that are understandable by collection units or agencies. The purpose is to provide the collection agency with specific collection and reporting requirements which ensure that the right data is collected and reported promptly to the appropriate user. When developing reporting requirements, the specific information that must be obtained, the assigned priority, and the origin of the request are considered.

The commander, or other originators of information requirements, may need the information by or at a specific time, or upon the occurrence of specific events. For example, a onetime report on the conditions of a river bottom may be required by a specified time. Reports of other enemy activities such as movement along particular roads may be required periodically. By SOP, reports of artillery, nuclear activity, the identification of new units, and similar items may be required as obtained. Periodic negative reports pertaining to certain activities also may be required. Reporting times are critical as they represent the time the requested information must be available if it is to be used. (An exception to this is the reporting of combat information.) In many cases, collection requirements not completed by the specified time are automatically cancelled. Care must be taken to establish accurate reporting time requirements, to preclude a collection requirement being cancelled too soon.

Combat information is reported to the requester or user as soon as it is collected, using the most direct means available. When developing reporting requirements

for combat information, the first task is to identify to which recipients collection units should report. Secondly, a determination is made as to what reporting requirements are necessary for reporting combat information for intelligence processing purposes. This may involve a different level of detail. Usually, reporting combat information should follow SOP.

Requesters should not ask for more detail than necessary to fulfill the SIR. This is especially critical when requesting information for use in target development. Otherwise, valuable time may be wasted collecting unneeded data. This ties up collection and delays the delivery of intelligence and targeting data.

Conversely, insufficient detail may not answer the SIR. This could result in the inefficient use of collection assets and failure of the mission.

Reporting requirements must include the identity of all units and headquarters requiring the information. Commanders who do not receive the intelligence they need at the specific time may miss a fleeting opportunity to catch the enemy at a disadvantage. Once determined, information and reporting requirements influence the selection of specific collection units and agencies.

Determine Resource Capability and Availability

The selection and tasking of organic and supporting collection units and the formulation of requirements for higher-echelon support require a basic knowledge of the units, agencies, and sources that can provide information. The following chart defines sources and agencies and shows what units and activities fit into each category.

Before a particular unit or agency is selected to exploit a specific source, a determination must be made as to what assets are both available and capable of collecting the information needed. This includes assets in organic collection agencies and those at higher echelons.

Capability. Asset capabilities must be known by the collection manager. These include factors such as frequency ranges for ESM systems, other system ranges, aircraft mission duration, mobility, linguistic capabilities, and other similar factors. This knowledge is used to determine which asset is capable of collecting information that will answer SIRs. A profile of system capabilities is provided in the DOD Capabilities Handbook. HUMINT resource capabilities must be obtained from the parent organization.

Availability. For organic or attached agencies (such as the MI brigade at corps) the collection manager needs to know the collection capability and the percentage of that capability available at a given time. For example, he must know the number of SLAR missions the MI battalion (AE) can fly within 24 hours, the percentage of operational noncommunications collection systems, the percentage of interrogators available, and so on.

For higher echelon resources, it is necessary to know the number of resources allocated and the approximate availability. For example, the division must know what EW support will be provided by corps and the number of OV-1D missions available to support the division in a specified period.

Selection. Once the available resources have been identified by unit and type, potential units are selected for each information requirement. This selection is made by comparing each available unit's resources against the collection requirement, based on five critical selection factors:

- ☐ Range.
- ☐ Timeliness.
- ☐ Technical characteristics.
- ☐ Environment (terrain and weather).
- ☐ Enemy.

A unit's resources are evaluated by the collection manager to ensure that the unit is capable of collecting the required information. The intent is to avoid tasking units with missions beyond their capability. In MI TOCs, operations personnel perform the same general comparison in the process of assigning a collection requirement to a specific asset.

SOURCES AND AGENCIES

SOURCES

A source is a person, system, or activity from which information is originally obtained. Source may or may not be under friendly control.

AGENCIES

An agency is any individual or organization which exploits a source to collect and/or process information.

COMMON SOURCES

- Captured enemy documents and material
- Enemy electromagnetic emissions
- Shell and missile fragments
- Contaminated areas
- Radioactive material
- Weather forecast reports
- Studies/ informants
- Civilian agencies
- Recovered US military
- Displaced persons
- Enemy activities
- Local residents
- Nuclear bursts
- Refugees
- Sounds
- Imagery
- Craters
- Odors
- Duds
- Maps
- EPW

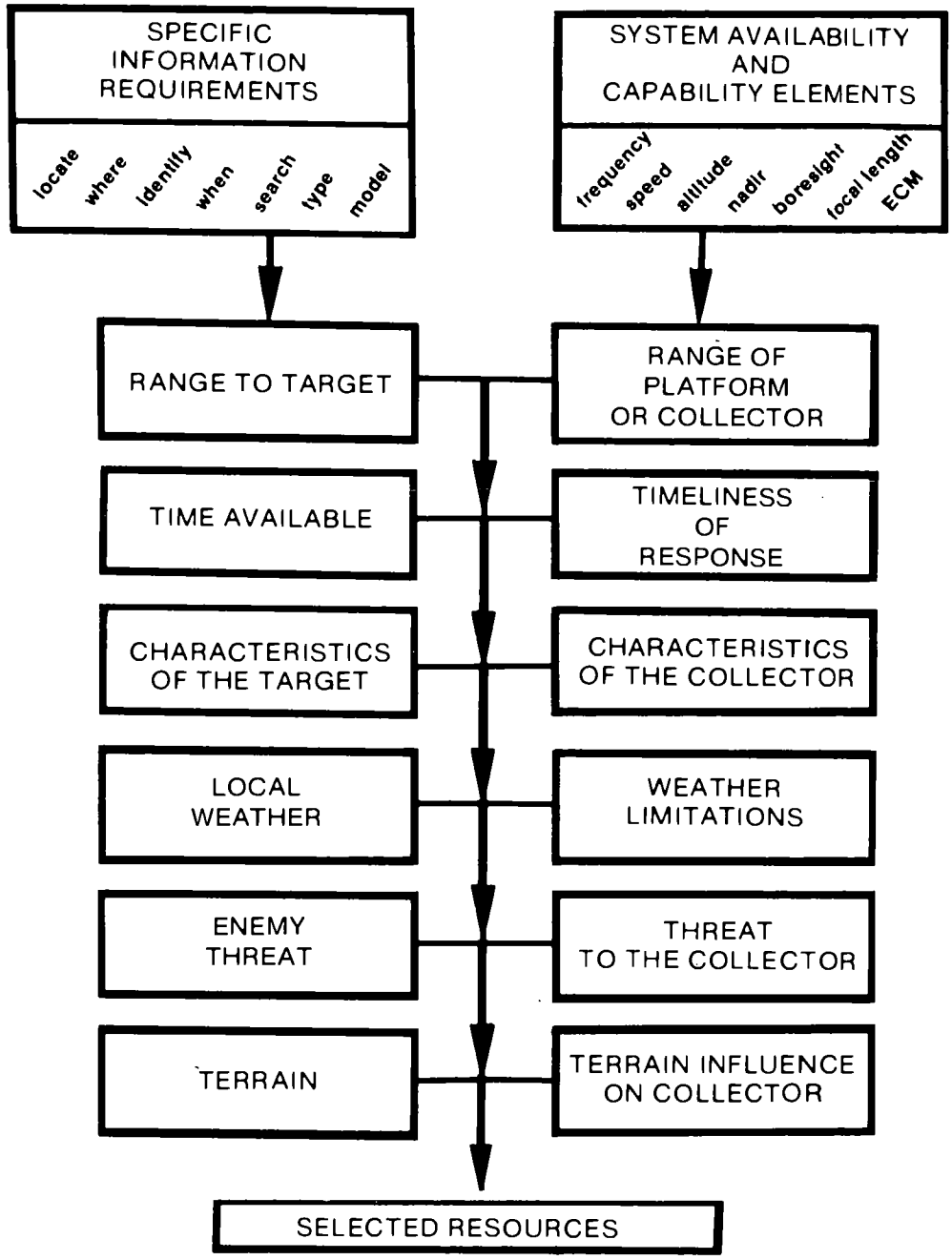
COMMON AGENCIES

- Lower and adjacent commands
- National intel agencies
- Civil affairs units
- Chemical units
- Engineer units
- Terrain teams
- Weather teams
- Other services
- Troops
- Cavalry
- Military police
- PSYOP units
- Allied intel
- ADA units
- CSS units
- INSCOM
- CI teams
- S&T Intelligence teams
- MI units
- Artillery
- Patrols
- Interrogation teams

The following illustration shows the correlations between specific SIRs and systems availability and capability.

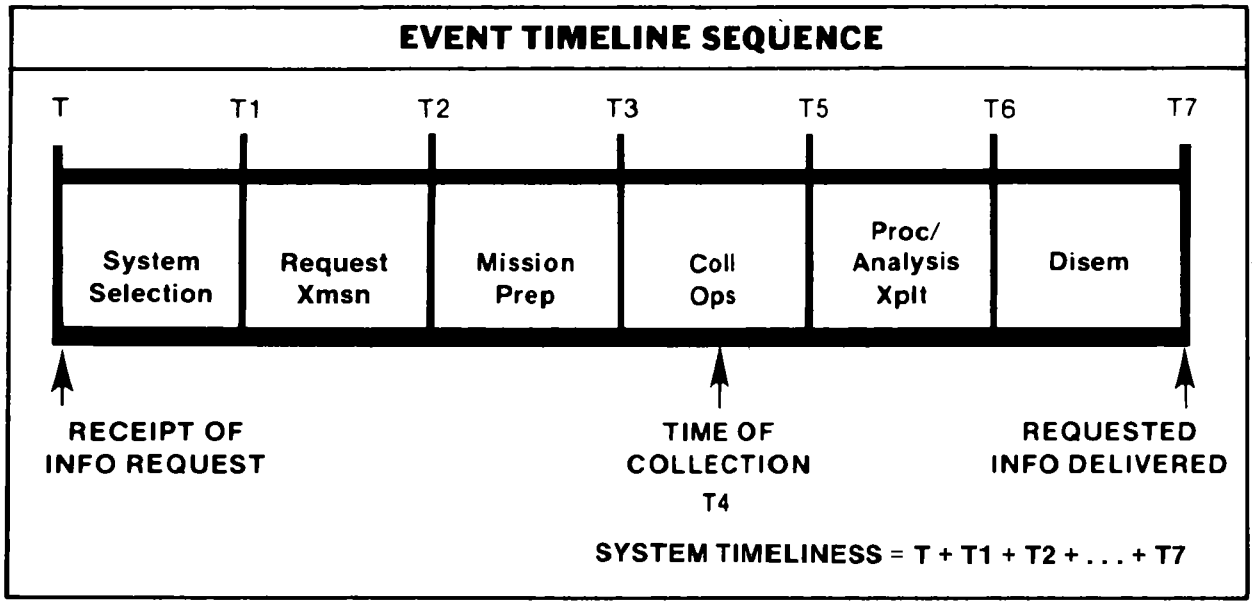
A system's capability is limited by its range. Range alone, however, may not be the determining factor. A GSR, for example, may be within range of a target but not able to detect the target because of an interruption by weather or terrain. In some cases, a system's range may be flexible, depending on its height above the ground, or be limited by the technical design of the intended target. Range may limit some HUMINT agencies such as patrols or scout units.

CAPABILITY/REQUIREMENT CORRELATION



Other HUMINT assets, such as interrogators are seldom affected by range considerations.

System timeliness is defined as the period beginning when an information request is received and ending when the information is delivered to the requester. The events shown in the following graph depict the general timeliness sequence that must be considered during any system capability



assessment. System timeliness is the sum of times from T to T7. Times required to complete each of the events shown in the graph should be calculated or estimated for each available system based on the tactical situation and the local SOP. Times will vary, depending on mission priority assigned, specific system availability for the collection requirement, and related information processing and dissemination means.

Timeliness is also affected by dependence on communications not included as part of the collection system. Tasking and reporting must flow over communications links that are highly vulnerable to enemy action, limited by range, and difficult to maintain during rapid displacement. Although the agency selected may be perfectly capable of acquiring the information needed, reporting may be delayed by communications problems.

Many surveillance systems operate nearly continuously over wide areas, providing I&W and tipoff information. Since they may not require additional tasking, the timeliness sequence to consider begins with those events that follow T4 in the graph.

Collection managers should consider constructing similar bar graphs using local data to provide a quick reference for the system selection process.

The technical characteristics of a system must be examined in detail to ensure that it has the capability to fulfill the collection requirement.

The location accuracy of a system is a technical characteristic that can be extremely important to the commander. IMINT systems are characteristically accurate since a direct association can be made between the imagery collected and corresponding map coverage. In cases where maps are available, location accuracy is limited only by the accuracy of the maps used and the competence of the analyst. Additionally, various computerized systems have been developed that are capable of identifying the coordinates of a point on imagery.

SIGINT and ESM systems do not have the inherent geographic accuracy of IMINT systems. Their location accuracy is limited by electromagnetic propagation factors and an inability to correlate collected data to specific map reference points. Emitter location accuracies are enhanced by multiple intercepts and LOB on the target transmitter by a group of systems working in concert. The correlation of data collected from all sources using templating and other analytic techniques will improve location accuracy.

The importance of location accuracy depends on the planned use of the information. Information collected for targeting purposes requires greater location accuracy than information collected for answering more general PIR and IR. The intended use of the needed information must be known to determine the location accuracy needed.

Correlation. Correlation of range, timeliness, and technical characteristics will provide a preliminary list of systems that—

- ☐ Are within the required range of the target.
- ☐ Can respond within the time required.
- ☐ Have the technical capability to collect the desired data.

Select Collection Resources

After availability and capabilities are determined, units and agencies are selected and tasked to acquire and report information. Selection of specific units is influenced by the effects enemy, weather, and terrain may have on the resource's ability to collect the required information. During this process all units are considered for tasking against every requirement. Capable assets are selected by a process of elimination.

Various procedures may be used to select the unit to collect specific information. One procedure is to use a selection worksheet prepared in a format similar to the one in the following illustration. In many cases the worksheet may be preprinted with current resources listed. It is used to consider the major factors determining the capability of an asset to satisfy specific information requirements.

The collection manager begins the unit and agency selection process by listing all available units and resources along the left-hand column of the worksheet. Next, the specific information requirement and its key elements are entered on the top of the form.

Asset capability then is considered in light of each of the capability factors. For example, since the first IMINT asset on the worksheet is the OV-1D MOHAWK, the initial determination would be whether the OV-1D is ***range*** capable of satisfying the requirement. The ***target range*** listed at the top of the worksheet is used to determine if the OV-1D can meet that requirement. This can be done by reviewing the system description for the OV-1D. When a system is considered incapable in any area, it is no longer considered. This procedure is repeated for each system capability and environmental factor.

At this point, the procedure is time consuming if followed precisely. In practice, however, there are many shortcuts. To explain these shortcuts, it is necessary to first examine the asset scoring procedure.

As each asset or factor combination is considered, a mark is entered on the unit selection worksheet to identify the capability of that asset against that factor. One of three marks is used:

\+ = fully capable
0 = marginally capable
\- = incapable

A single dash under any factor eliminates that asset from consideration. Often the experienced collection manager can readily identify one or more asset or factor combinations that would result in an incapable rating. This constitutes a considerable saving of time, since a large percentage of the incapable assets can be eliminated by a quick inspection of the asset or factor combinations. When there is doubt about the capability of an asset, refer to the appropriate documents.

Enemy capabilities are considered during the system selection process. In many cases, enemy action will restrict the use of, or reduce the effectiveness of, a particular system. For example, when the enemy has air superiority, the use of aerial assets may be restricted to avoid excessive losses. Heavy concentrations of enemy air defense missiles on the FLOT may increase stand-off distances and thereby reduce the effective range of aerial systems. During periods of enemy radio and radar silence, the use of ESM may produce little information. By staying abreast of the tactical situation, attention is focused on agencies with collection resources that have the best possibility of completing the collection mission.

UNIT
ASSET SELECTION WORKSHEET

Org. V Corps
Reg. No. 2
DTG: 050100Z May 82
Collection Mgr: Brown
Target Range: 80km

Specific Info Requirement: Vehicle movement between coordinates AC091061 and AC201085
Time Required: 052200Z May 82
Characteristics:

ASSETS	Capability Factors			Environmental Factors			Capable	Remarks
	Range	Time-liness	Char-acter-istics	Wea	Threat	Terrain		
IMINT								
OV-1D SLAR	+	+	+	+	+	+	+	
RF-4 Photo	+	+	+	+	+	+	+	
ELINT								
QUICKLOOK	+	+	-					
COMINT								
GUARDRAIL	+	+	0	+	+	+	0	
QUICKFIX	-							
HUMINT								
LRSU	+	0	+	+	0	0	0	

ASSETS SELECTED:

IMINT: OV-1D SLAR, RF-4 PHOTO
ELINT:
COMINT: GUARDRAIL
HUMINT:

UNIT
ASSET SELECTION WORKSHEET

Weather plays a particularly important role in the selection process. Weather can affect both the capability of a system to collect data and the exploitation of the data collected. For example, heavy rain or cloud cover directly limits the collection of imagery.

Terrain also influences the selection of systems. Mountainous terrain masks enemy movers from moving target indicator (MTI) systems. Mountains, hills, and built up areas attenuate radio waves, thereby reducing the effectiveness of SIGINT systems. Heavily forested areas may obscure enemy movement.

All outstanding intelligence requirements and the tactical situation are considered in collection planning. However, certain collection factors must be considered before tasking orders are sent. These factors include resource integration, cuing of one system by another to build the required data package, and the selection of a proper resource mix and redundancy to increase the probability of completing the collection mission successfully while defeating enemy deception attempts.

The degree to which newly developed collection requirements can be integrated with current or planned actions will, to a large extent, determine the efficiency of the overall collection effort. As a goal, every attempt is made to combine new collection requirements with ongoing actions to employ the fewest resources. This decreases risk while increasing the overall collection capacity available. Before requesting additional missions, the following possible alternatives for integration of collection requirements with planned or ongoing missions are considered:

- Tasking adjustment. Examples of this would be adding new collection requirements which do not conflict with ongoing missions, diverting missions in process to collect against a higher priority target, and changing planned collection operations to substitute higher priority targets.
- Exploitation adjustments. This consists of modifying exploitation instructions to reflect the evolving situation and the need for additional exploitation. An example of this is the paying of increased attention to a particular area covered during routine surveillance missions.
- Reporting and dissemination adjustments. This consists of modifying the reports distribution plan to accommodate requesters who can be satisfied by a particular ongoing collection operation.

New tasking is prepared as a last resort when other means of collection are neither possible nor feasible.

The benefits of using one resource to cue another should not be overlooked. ***Cuing*** involves the use of one asset, usually a wide-area-coverage surveillance system to provide necessary targeting information to a more accurate point target system.

In some cases, a cuing arrangement is essential to mission accomplishment. For example, the requirement to detect and accurately locate antiaircraft artillery (AAA) within a large target area using continuous photo penetration missions would be very risky and inefficient. The use of standoff ESM systems to report AAA emitters, locations, or LOB followed by penetrating photographic sensors would be timely, more effective, and less costly. MI brigade and battalion S3s are the focal points for cuing respective corps and division resources. However, the collection manager plays a critical interface role in providing tipoff data from higher echelon systems that do not have a direct communications link with these organizations.

In some tactical situations, it may be beneficial to plan for collection against a target using a combination of similar resources ***(redundancy)*** or of differing resources ***(mix).*** Redundant tasking may be required against high-priority targets when the probability of collection is too low for any one system. Tasking a number of ESM resources to target a designated emitter over specific periods of time improves the probability of successful collection. This is true especially when the emitter operates

intermittently. On the other hand, employing a mix of systems not only increases the probability of collection but also provides more complete information. For example, IMINT may detect and locate an enemy tactical force while SIGINT and HUMINT supply its identity, organizational structure, and indications of future plans. Employing a mix of systems is always desirable if the situation and available resources permit it. Mixing systems also uncovers deception attempts by revealing discrepancies in information reported by different collectors.

Whatever resource mix or redundancy is considered, the mission integration considerations described previously still apply. Therefore, any tasking that places greater demands on the limited resources available must be clearly justified by the potential intelligence gain.

Other factors that are considered before tasking a unit or agency are capability, suitability, and balance.

An agency must be physically capable of providing the desired information in a timely manner. For example, an armor unit in reserve is not asked for identification of units in contact, nor is an OV-1D SLAR asked for targeting information about movers that can be obtained by an AN/PPS-5. Neither is an AN/PPS-5 tasked for targeting information about deep movers.

Suitability of the agency or resource impacts on the selection process. Every effort is made to select an asset that provides the greatest probability of success and at the same time will not provide inappropriate overkill. The collection task assigned to a unit must be compatible with its primary mission. Only the agencies best suited to furnish the desired information are used. For example, information most readily acquired by dismounted patrols should be obtained by infantry or cavalry units rather than MI units. Economy of personnel and materiel also is considered. There are many units and agencies, other than MI units, which can be tasked for information.

Within the limits imposed by other considerations, the collection workload is balanced among MI units and other units. Balance, however, is a very minor consideration when compared with the importance of other factors.

Task Collection Resources

Following agency selection, intelligence requirements tasking is prepared. Intelligence requirements tasking is directed toward a unit or agency rather than a specific asset. However, because of the completed collection planning process described above, the collection manager is able to direct tasking to a unit with assets capable of collecting the information.

The purpose of intelligence requirements tasking is to provide the selected unit with a specific requirement, but not with specific instructions for carrying out the mission.

Requests for Intelligence Information. RIIs are generated by a subordinate command to obtain intelligence or information collection support for needs that exceed organic capabilities. Requests for information are prepared using the RII or a similar narrative format. Requests received that exceed organic requirements are always consolidated and forwarded to the next higher echelon as RII. A request reaching corps is at the highest echelon of tactical RII processing. Regardless of the echelon originating the request or requirements tasking, the tasking is prepared to indicate the degree of urgency and the type of request being made. Requests are assigned priorities depending on criticality and the timeline specified by the requester.

At corps and division, intelligence requirements tasking is directed toward MI commanders and commanders of other elements of the combat force capable of collecting the information. Priorities are assigned to each intelligence requirements tasking based on those previously established. When new intelligence requirements tasking is generated in an ongoing operation, high-priority requirements may preempt lower-priority missions previously tasked.

Besides tasking directed to subordinates, requests may be sent to higher or adjacent commands. Intelligence collection requirements, which exceed the capabilities of organic assets, are prepared as specific

requests for information using the RII. Requests may include information concerning adjacent areas of interest, the command's own area of interest at ranges beyond the capabilities of organic resources, or other information not obtainable by the command. Procedures established by SOP and the Joint-Tactical Exploitation of National Systems (J-TENS) manual are followed for requesting support from higher echelons and national systems.

There is also a danger of reported information taking multiple paths to the ASPS and confirming itself as if the information originated from two or more sources. An example of this is a tactical report (TACREP) from the TCAE that is also in a brigade intelligence summary (INTSUM). To the analyst receiving these reports it appears that the information originated from two sources. To avoid this, the collection manager and analysts in the ASPS must validate reports by identifying the source and time of the information.

Tasking Documents. Tasking documents are used to levy intelligence requirements on the various agencies. In the case of organic systems, this involves orders to units in accordance with command policy and SOP. As a general rule, intelligence requirements tasking at both corps and division is done through either fragmentary orders, the intelligence annex to the OPORD, SOP, or the RII. Request formats for support from national systems are specified in the J-TENS manual.

Systems controlled by a higher headquarters, other services, or national agencies respond to approved requests for information passed through appropriate channels. The channels used depend on the agency and the requirement, the agency receiving the requirement, and command procedures.

The intelligence annex is standardized and has a more rigid format than other annexes. The purpose of the intelligence annex is to—

- ☐ Issue instructions to subordinate commanders and requests to higher headquarters to collect information before or during the initial phase of an operation.
- ☐ Provide intelligence orders or guidance, which varies from SOP, for handling of EPWs, refugees, captured documents and materiel during the operation, and NAI particularly important to the issuing headquarters.
- ☐ Confirm the orders and requests for information that have been made in fragmentary form and that are still current at the time the annex is issued.
- ☐ Preserve brevity, clarity, and simplicity in the body of the order.
- ☐ Amplify an order when information is of limited application to the entire command or is primarily technical in nature.
- ☐ Disseminate information and intelligence at the start of an operation and when there is a major change in mission.

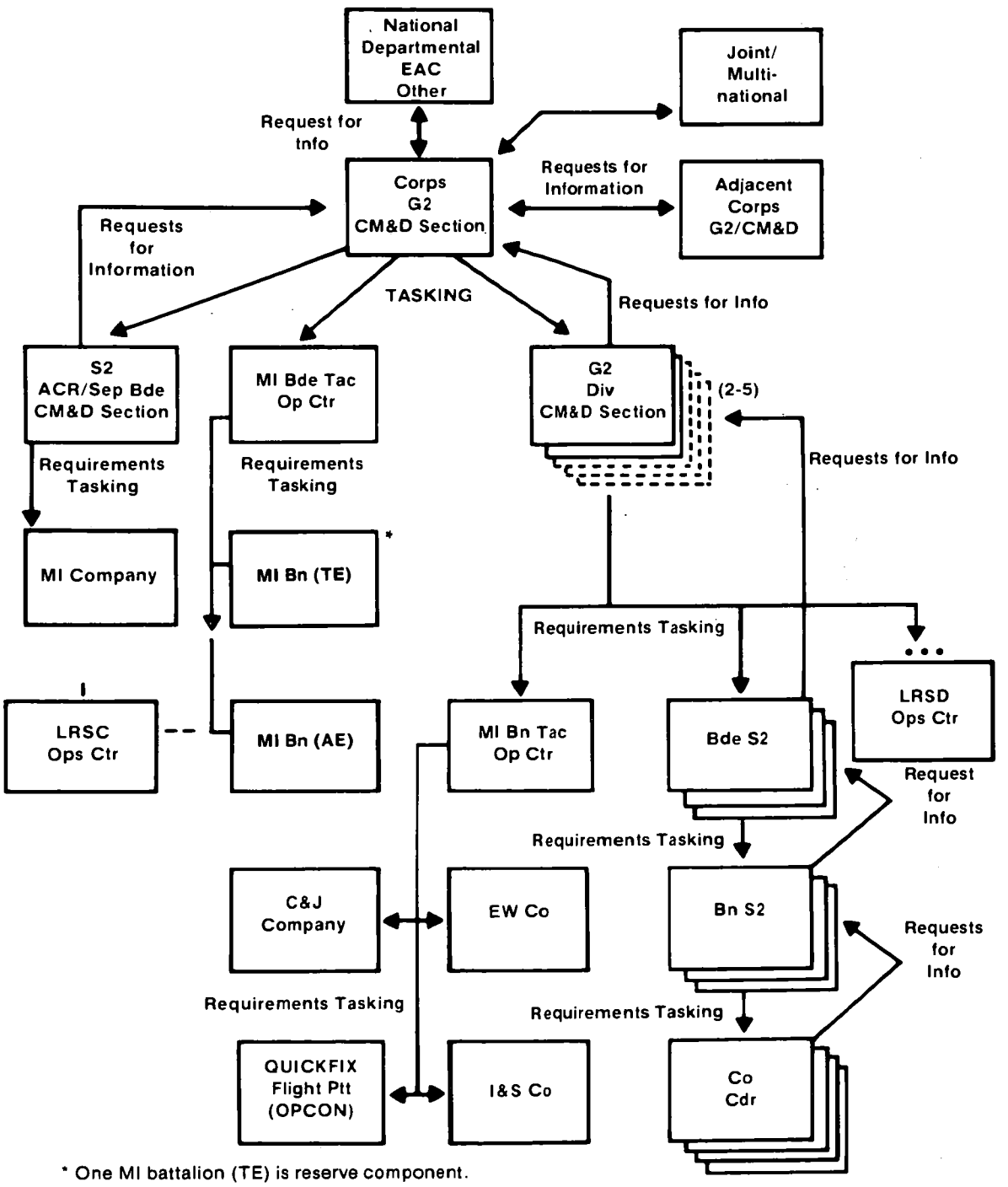
Instructions on how to prepare the intelligence annex are contained in Appendix C.

Paragraph 3 of the intelligence annex, intelligence acquisition tasks, implements the collection plan. It contains a complete list of current orders and RII. Except for collection orders which are a part of the unit SOP, previously issued taskings not repeated in the intelligence annex are automatically cancelled. When intelligence orders and requests are lengthy, they may be placed in an appendix to the intelligence annex.

Fragmentary orders (FRAGOs) are used most frequently because information requirements continually change. OPORDs have a prescribed format, but, FRAGOs do not. Those elements found in a complete order are omitted when they have not changed, are not essential, or are unavailable or incomplete at the time of issue. An example of a FRAGO is provided in FM 101-5.

Tasking Flow. Corps is the point where national, departmental, joint, multinational, and tactical levels are integrated. Requests beyond the capability of corps or division systems are passed by the collection manager to EAC, national level, or other services for action. Conversely, EAC,

TASKING FLOW



* One MI battalion (TE) is reserve component.

national, and other services task corps and division systems through corps. The corps collection manager incorporates these requirements into collection planning as other requirements that must be answered. RII and tasking flow are shown in the illustration on page 3-34.

Regardless of the echelon originating requirements tasking, the tasking is prepared according to a number of general considerations. Requests are normally categorized by degree of urgency and type. The degree of urgency determines the time constraints placed on the request. Requests are assigned a priority depending on criticality and how soon the information must reach the requester. Requests for information forwarded to national systems should specifically state the time the information is required by the user.

Anticipated requirements to collect information are best met by preplanning and advance scheduling. Preplanning is especially important to satisfy basic requirements such as weather, terrain, and enemy OB. Satisfaction of these preplanned requests requires thorough coordination with the ASPS, planning, and consolidation.

Preplanning often provides the user with more responsive support by allowing mission planners and commanders sufficient time to schedule the required collection mission. This is particularly important when advanced systems are coordinated at the national level. These systems often require considerable programing to effect collection. Preplanning also offers greater flexibility for system coordination in selecting the most efficient collection means and consolidating collection requests. As a practical goal, as many requirements as possible should be preplanned. In addition, every effort should be made to submit requests as early as possible.

Immediate requests are limited to unforeseen requirements for information of immediate value to the tactical commander. This can often provide specific information relative to satisfying the PIR. However, care should be taken to ensure that only need-to-know items are submitted as immediate requests and that these items have a definite tactical value. Targeting information, composition, and disposition of committed and reinforcing forces, and disposition of highly mobile air defense systems are a few examples that could serve as the basis for immediate requests.

Surveillance is the systematic observation of aerospace, surface or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. Surveillance is normally used to gain information on the subject over a long period of time to note any changes that may take place.

Reconnaissance is undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy or to obtain data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. Reconnaissance is a directed effort to obtain information on a subject at a particular time.

Because of the interrelationship of reconnaissance and surveillance, the same assets used to execute reconnaissance missions may also be used for surveillance tasks.

As noted above, surveillance missions are characterized by a systematic, although not necessarily routine or constant, watch of persons, places, or things by HUMINT, IMINT, or SIGINT resources. Surveillance missions are usually preplanned and are particularly suited to—

- ☐ Cover large areas rapidly and repetitively.
- ☐ Minimize risk to the collector.
- ☐ Observe or detect changes on the enemy side of the FLOT.
- ☐ Cue other collectors for more detailed coverage.

Planning for surveillance operations is conducted after determining the general mission of the tactical force. Surveillance missions are often developed as a joint effort involving all of the intelligence organizations having an interest in the

same area of operations. This is due to the limited availability of surveillance systems and the large number of overlapping requests that could be generated in a joint or combined operation.

A reconnaissance mission seeks to obtain information by visual or other detection means and is characterized by limitations of coverage to one or more specific target areas at a particular time without the requirement for systematic coverage. Reconnaissance missions are conducted by HUMINT, IMINT, and SIGINT resources and are designed to—

- ☐ Collect specific, detailed information at a particular location and time.
- ☐ Support current or planned operations.

Most reconnaissance requests are preplanned before the operation. However, once operations begin, many reconnaissance requests will be immediate. The time constraints of the typical reconnaissance request will not allow for elaborate planning or coordination. A request that would be classified as a requirement for a reconnaissance mission might be for urgent photographic coverage of a proposed helicopter LZ some distance beyond the FLOT.

Valid justification is particularly important for immediate surveillance or reconnaissance requests. This is critical if national systems may be required to collect the information. Such systems are in high demand, and the restructuring of programed national collection plans requires adequate justification.

Requests for support from national systems cannot be so easily categorized as preplanned or immediate, or as surveillance or reconnaissance. This is, in part, because of the many national agencies involved and the diverse missions and performance characteristics of individual collection resources. In the case of the national IMINT, the collection manager must be familiar with the mission, the commander's intent, the OPLAN, and the Imagery Reconnaissance Directives List (IRDC) associated with the area of interest.

The national SIGINT system also operates against long-term, standing requirements. In the case of SIGINT, the tactical commander's crisis or combat requests will be termed time-sensitive and handled expeditiously.

Requests for national HUMINT support ultimately go through DIA after EAC coordination procedures have been completed.

Evaluate Reporting

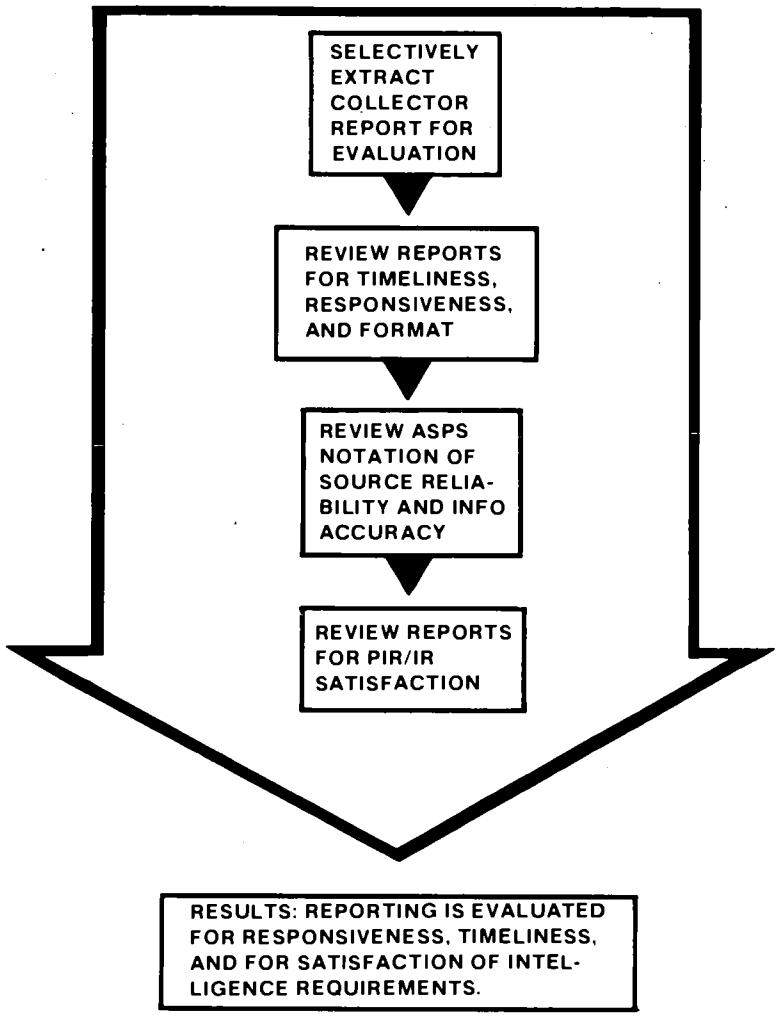
Collection management does not end with the issuance of orders and requests. Steps are taken to ensure that orders and requests are received by the collection agencies and that they are clearly understood. Collector and ASPS reports are monitored throughout the collection process to ensure that intelligence and information are reported to the right user in a timely manner. Reports are selectively extracted for sampling and are reviewed for—

- ☐ Timeliness. The time the event took place is compared to the time the event was reported. This comparison reveals delays and possible problems with the reporting of collected information.
- ☐ Format. Reports are checked to see if they contain the proper addressees and data elements.
- ☐ Responsiveness. Reports are checked to see if the information being reported satisfies the commander's PIR and IR. The following illustration shows the report evaluation process.

Update Collection Plan

An important aspect of the collection management process is the cancellation of intelligence requirements tasking and the updating of the collection plan. The collection manager must always be able to cancel requirements to make room for new high-priority tasks in response to the commander's operational needs. For example, if an armored division commander is moving north and suddenly sees an opportunity for a flanking maneuver to the west, collection management must have the flexibility to provide responsive support. It is as important to be able to cancel a requirement as it is to levy it in a situation of limited collection resources.

REPORT EVALUATION PROCESS



When requested information is reported back to the CM&D section, it must be matched with the collection requirement it satisfies. The collection management effort is only effective if it can match incoming information with collection requirements. The incoming information may not come from the collector that was tasked, and may, by coincidence, partially satisfy another requirement. If so, the old collection requirement, which is now broader in scope than necessary, must be rewritten to fill the specific void.

Collection agencies must be notified of modifications to collection requirements. The modified requirement may also require a new priority and an adjustment to its time

specifications. Each time the requirement is modified or satisfied, the collection plan is updated.

Updating the collection plan is a continuous process requiring close attention. It is updated upon—

- ☐ Fulfillment of PIR and IR.
- ☐ Receipt of new PIR and IR.
- ☐ Modification of existing PIR and IR.
- ☐ Changes in enemy, weather, or terrain which dictate a change in tasking.

The ASPS determines when PIR and IR have been satisfied. When it is determined that a requirement has been satisfied the CM&D section is notified immediately. Satisfied requirements are removed from the collection plan and collection actions against those requirements cancelled. This frees tasked resources for other collection missions.

Fulfilled PIR and IR also are compared with the collection plan to determine unsatisfied requirements. Unsatisfied PIR and IR, related indicators, and specific information requirements are reviewed to determine if—

- ☐ The information requirement is still valid.
- ☐ Further tasking is necessary to fulfill the requirement.

Fulfilled and unsatisfied requirements no longer applicable are deleted from the collection plan. Often during the analysis process, the ASPS identifies voids in the intelligence data base. The collection manager is notified that adjustments are needed to the collection plan. When notified of a void in the collection plan, steps are taken to update the collection plan and initiate the appropriate collection action.

Collected information is reported to the CM&D section. As incoming reports are received they are noted on the collection plan and forwarded to the ASPS for processing. During information processing, data to support situation development are obtained.

PROCESSING

In the situation development process, intelligence is developed in response to the commander's information and operational needs. It is then evaluated and integrated into an all-source product to provide a continuing estimate of enemy intentions. Through processing, situation development provides all-source intelligence for tactical decisions.

Processing is the transformation of information into intelligence and targeting data. The objective of information processing is to—

- ☐ Answer the commander's requirements regarding enemy movers, emitters, shooters, sitters, capabilities, vulnerabilities, probable courses of action, intentions, and terrain and weather in the battlefield area.
- ☐ Develop the targeting data required for effective attack of mover, emitter, shooter, and sitter targets.

Processing is facilitated through the use of intelligence data bases.

INTELLIGENCE DATA BASE

The intelligence data base provides the basic information required in the situation development process. The data base is created for potential contingency areas before hostilities. It is a combination of what we think we must know, what we do know, and what we don't know about the enemy, weather, and terrain. It—

- ☐ Is established and maintained by the ASPS or BICC.
- ☐ Focuses on specific areas.
- ☐ Contains information on enemy, weather, terrain, sociology, politics, training, economics, psychology, and other factors.

The following matrix depicts, by echelon, data base information requirements.

The intelligence data base is created by accomplishing a thorough, in-depth IPB analysis. Existing OB, to include technical data, is used to create the initial data base. A thorough research of information (from DIA, NSA, CIA, INSCOM, country studies,

DATA BASE NEEDS BY ECHELON

CATEGORY OF INTELLIGENCE		BN	BDE	DIV	CORPS	EAC
Identification, organization, weapons, equipment, location, tactical deployment, movement, and strength of--	Companies	x	x			
	Battalions	x	x	x		
	Regiments	x	x	x	x	
	Divisions		x	x	x	x
	Armies			x	x	x
	Fronts				x	x
Logistics information about--	All classes and types of supply			x	x	x
	Requirements			x	x	x
	Procurement				x	x
	Distribution			x	x	x
	Transportation			x	x	x
	Installations			x	x	x
	Terminals				x	x
	Evacuation and salvage				x	x
	Maintenance			x	x	x
Unit effectiveness Information about--	Personnel strength	x	x	x	x	x
	Amount and condition of weapons / equip	x	x	x	x	x
	Status of training	x	x	x	x	x
	Efficiency of personnel	x	x	x	x	x
	Length of time unit in combat	x	x	x	x	x
	Traditions and past performance	x	x	x	x	x
	Personality traits of unit commander		x	x	x	x
	Status of technical and logistical support of unit	x	x	x	x	x
	Morale, health, discipline, political reliability	x	x	x	x	x

(continued on next page)

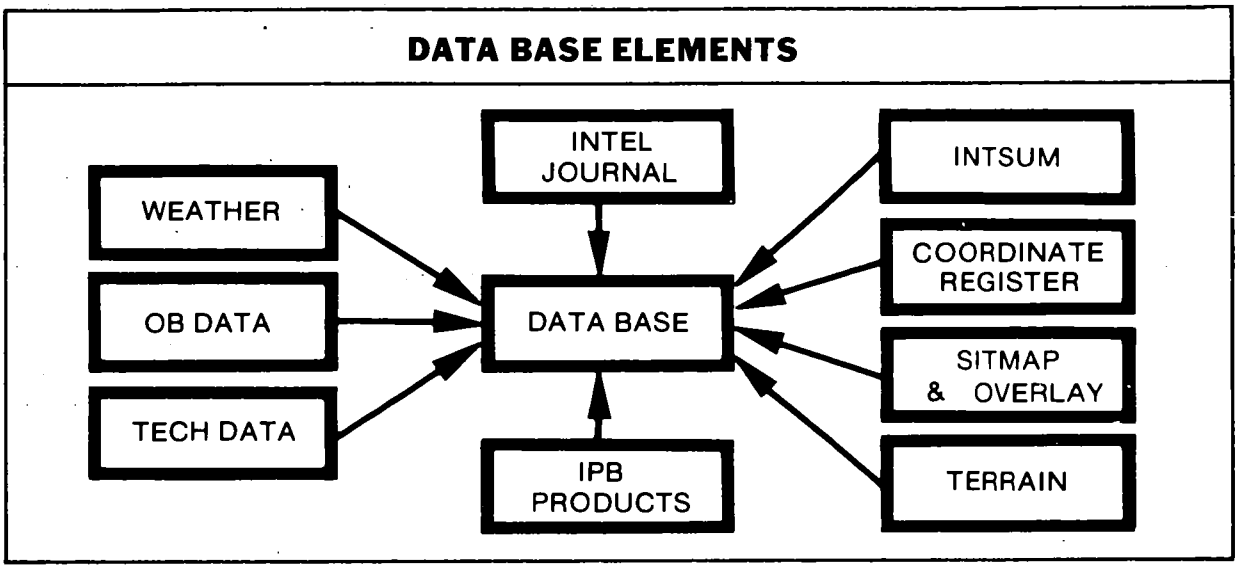
DATA BASE NEEDS BY ECHELON (CONTINUED)

CATEGORY OF INTELLIGENCE		BN	BDE	DIV	CORPS	EAC
Terrain information about—	Obstacles	x	x	x	x	
	Rivers	x	x	x	x	x
	Bridges	x	x	x	x	x
	Fords	x	x	x	x	
	Ports and harbors				x	x
	Observation and fields of fire	x	x	x		
	Concealment and cover	x	x	x		
	Key terrain	x	x	x	x	
	Ground and air avenues of approach	x	x	x	x	
	DZ and LZ		x	x	x	x
	Barriers and fortifications	x	x	x	x	x
	Trafficability	x	x	x	x	
	Roads	x	x	x	x	x
	Built-up areas		x	x	x	x
Weather information about—	Temperature	x	x	x	x	x
	Ground visibility	x	x	x	x	x
	Surface winds	x	x	x	x	x
	Precipitation	x	x	x	x	x
	Snow and ice cover	x	x	x	x	x
	Winds aloft	x	x	x	x	x
	Cloud cover	x	x	x	x	x
	Light data	x	x	x	x	x
	Severe weather	x	x	x	x	x
NBC information about—	Location of nuclear explosions and yield	x	x	x	x	x
	Nuclear and chemical weapons	x	x	x	x	x
	Direction of fallout	x	x	x	x	x
Electronic technical data about—	Emitter nomenclature		x	x	x	x
	Emitter type		x	x	x	x
	Mode of emission			x	x	x
	Frequency range			x	x	x
	Location accuracy for DF		x	x	x	x
	Associated use-units or weapons		x	x	x	x

and current intelligence) should be done for data base preparation during peacetime.

After hostilities begin, the data base is maintained and refined to reflect all pertinent knowledge of the enemy, weather, and terrain in the friendly unit's area of interest.

The intelligence data base must be functionally organized for the intelligence production process to be successful. Organizing



the data base is done by separating information, either manually or by automation, into appropriate files. These files should consist of the intelligence journal, OB data, IPB products, and situation map (SITMAP). The number of files maintained should be determined by time and resources available. Elements of the data base are shown in the above illustration.

Intelligence Journal

The intelligence journal is a permanent, chronological record of each message or document entering or leaving the ASPS or BICC and may contain administrative data according to SOP. The journal provides a cross reference—a complete compilation of all incoming reports for purposes of future recovery. The journal covers a specified time, usually 24 hours, and is recorded on DA Form 1594.

The journal file contains the DA Form 1594 and incoming or outgoing documents collected during the specified time. Documents are posted with the corresponding journal entry number and filed in sequence. The journal is an invaluable tool during continuous 24-hour-a-day operations involving personnel shift changes.

Order of Battle Data

OB is the identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. In LIC campaigns involving irregular force units, auxiliary and underground elements are included in the OB data base. The OB data base consists of evaluated information on the enemy—

- ☐ Composition.
- ☐ Disposition.
- ☐ Strength.
- ☐ Training status.
- ☐ Tactics.
- ☐ Logistics.
- ☐ Combat effectiveness.
- ☐ Electronic technical data.
- ☐ Miscellaneous data.

Data is developed in many fields outside the scope of OB, but all intelligence is ultimately related to it. For example, S&T intelligence produces intelligence on the capabilities of weapon systems, but OB intelligence determines the effect of weapon capabilities and characteristics on enemy tactics, combat effectiveness, and organization.

OB files are cross-referenced and organized for rapid access and retrieval. They are kept current and used to identify gaps in data holdings. OB files provide a format for recording enemy combat losses.

Combat loss data, resulting from postattack assessment, provides input to compute enemy strength. Information concerning

strength provides indications of enemy capabilities and assists in determining the probable courses of action or options open to enemy commanders. A lack or a preponderance of strength has the effect of lowering or raising the estimate of the capabilities of an enemy force. Similarly, a marked concentration of units in an area gives indications of enemy objectives and probable courses of action. During peacetime, changes in the strength of potential enemy forces are important factors which indicate the enemy's intention to wage war.

IPB Products

IPB files contain the IPB templates described earlier in this chapter.

SITUATION MAP

The basic SITMAP provides a temporary graphic display of the current, known dispositions, and major activities of both friendly and enemy forces. The basic SITMAP provides a format for accurate notations of enemy forces relative to friendly boundaries.

The purpose of the intelligence SITMAP and all associated overlays is to contribute to sound tactical decisions. The primary intelligence uses of the SITMAP and associated overlays are to—

- ☐ Display the enemy situation and disposition.
- ☐ Provide a basis of comparison to determine the significance of newly received data pertaining to enemy forces.
- ☐ Provide a basis for briefings and intelligence reports.
- ☐ Focus attention on intelligence gaps which require redirection of the collection effort.
- ☐ Assist in determining patterns of enemy movement and probable courses of action.

Separate topical overlays are used in conjunction with the SITMAP, to display all other information regarding the enemy. The following are examples of the types of entries, made in accordance with FMs 101-5-1 and 21-31, that may be posted on the current SITMAP overlay to show enemy—

- ☐ Unit identifications.
- ☐ Unit locations including time of information.
- ☐ Boundaries.
- ☐ Location of major weapons systems.
- ☐ CPs.
- ☐ Logistics centers.
- ☐ Aircraft staging areas.
- ☐ LZs and DZs.
- ☐ NBC contaminated areas.

Posted information varies with the size of the friendly unit maintaining the SITMAP. For example, division SITMAPs will normally show the location of enemy units down to battalion level. Smaller elements of some critical enemy units, such as artillery, may be shown. If the presence of individual weapons is considered a decisive factor in a particular operation, they are shown. Reports of individual weapons and equipment can be critical to the analytical effort whenever such information would contribute to the identification and location of the unit to which assigned.

Electronic Order of Battle Overlay

EOB overlays are used to graphically depict communications and noncommunications emitters (radio/radar/jammer and so forth) and associated units, facilities, and activities which have been located through ESM or SIGINT. There will be many more emitters than units on the battlefield. To attempt to depict on one graphic all OB elements would quickly clutter a single 1:50,000 scale overlay. Therefore, it is recommended that a separate overlay be used for the emitter data elements listed below. Emitter types and signal parameters can be associated with particular units, in some cases, and aid the analyst in confirming or denying the presence of enemy units and activities. Not all the data elements listed will be known or will be appropriate for a single emitter. These elements may include—

- ☐ Emitter type.
- ☐ Modulation.

- ☐ Frequency.
- ☐ Unit identification or level of command.
- ☐ Weapons system association.
- ☐ DTG of observation.
- ☐ Journal number of message providing the data.

Other prolific collectors may require their own overlays to avoid map clutter. As an example, SLAR MTI reports may be posted on a single overlay to aid in the analysis of enemy movement patterns.

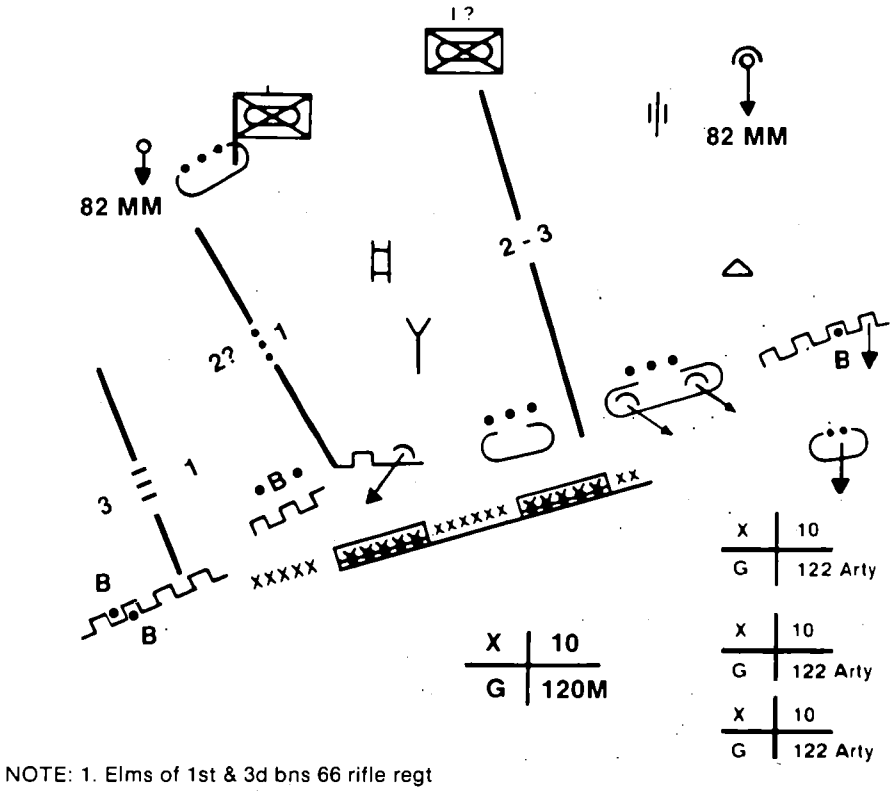
Collateral Overlay

The collateral SITMAP overlay is normally limited to SECRET information. All incoming information which meets the classification levels can be posted on the collateral SITMAP overlay. The term "collateral" applies only to the security classification. More than one collateral overlay may be necessary to allow for an uncluttered presentation and to facilitate functional integration.

Coordinates Register

The coordinates register, most effective at brigade and battalion, provides a means of noting intelligence associated with specific areas. It can be compactly formatted and easily carried. One such format is the loose-leaf notebook. Each page of the notebook

GRAPHIC STYLE OF COORDINATES REGISTER



NOTE: 1. Elms of 1st & 3d bns 66 rifle regt

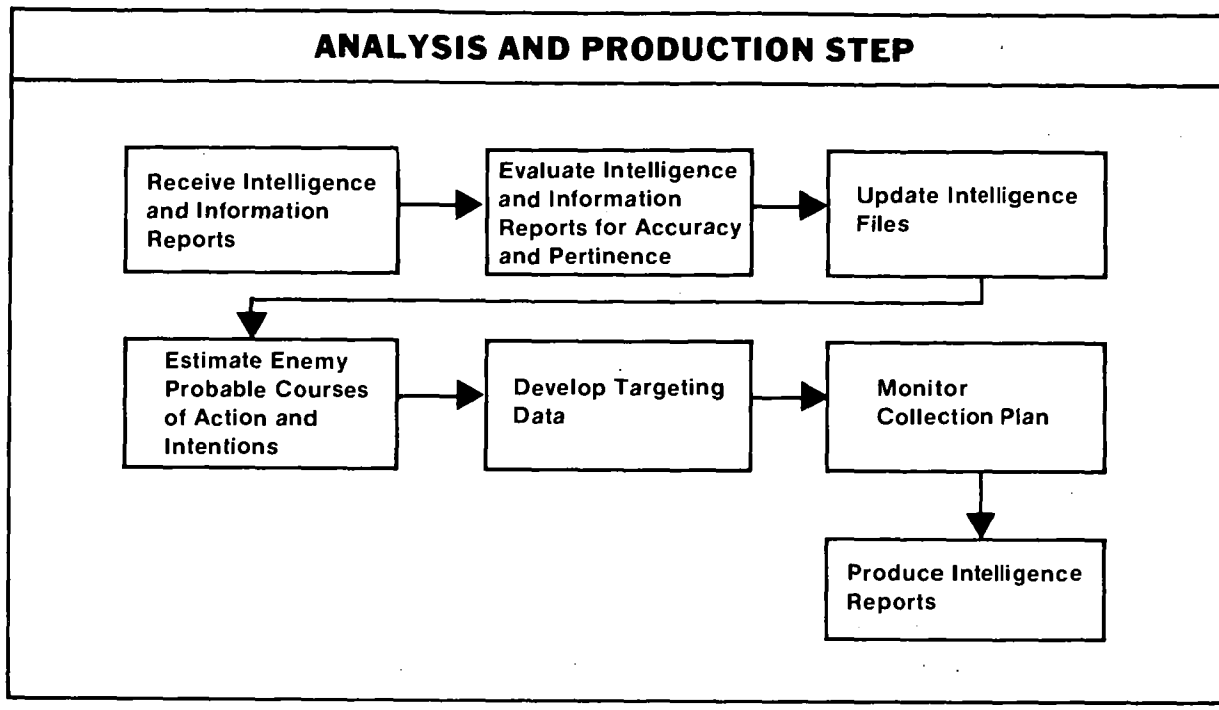
NOTIONAL STYLE OF COORDINATES REGISTER				
GRID SQUARE 2815				
ITEM	TIME	COORD	STATEMENT	NOTES
1.	092235	28381539	MG fired on recon patrol from A Co	Have next patrol check this area
2.	092318	?	Veh noise - Tk? - Heard direct N. of A Co OP #2 28321507	Ask air OP to look
3.	100600		Special OB report on wpns & fortifications	Div OB wants more info on wpns strength
		28021523 to 28141527	Trenches & bunkers	Same MG as yesterday? Check this!
		28141527 to 28221529	Wire	
		28611545 to 28781551	Platoon on line- has 2 MGs	
		28811551 to 29001599	Extensive trenches and firing pos	
4.	102335	28391530 to 28691541	B Co patrol repts wire and AP mines	New since 081800
5.	110600	28431588	Res unit (Co ?) in gen'l area	(From div PERINTREP)
6.	110630	28381557	Med tank spotted by lt plane	How many more???
7.	111320	28731584 and 28151564	Active mortars	
8.	120010	28611564	Flash from small cal arty not over 75	At? AA? Gun? Rclr or Bazooka? Ask higher HQ

pertains to a single grid square of the pertinent map area of interest. Recording of pertinent data can be by either written notation or a graphic portrayal. The preceding two illustrations are examples of both styles of notation.

INTELLIGENCE PRODUCTION PROCESS

The ASPS converts reported intelligence and information from the CM&D or subordinate units into all-source intelligence using a basic production process. The section receives data in two forms. The first is information; data which has not been subjected to correlation or analysis. The second is processed intelligence. Through the process illustrated below, both types of input are correlated and analyzed to give the ASPS further refined intelligence.

The following illustration provides an overview of the analysis and production process.

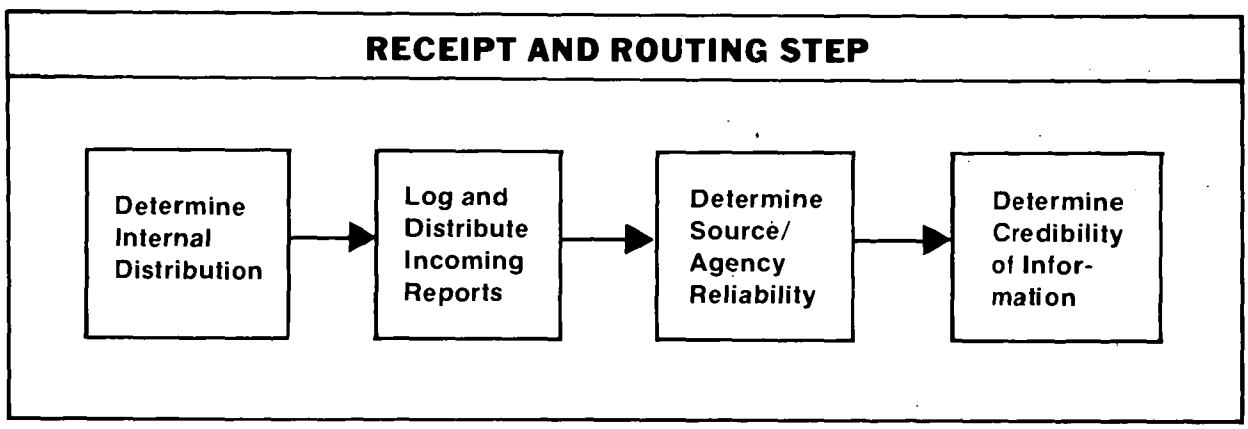


Receive Intelligence and Information Reports

The first step in the intelligence production process is the receipt and routing of incoming information. In this step information is logged in, checked for reliability, and distributed for further evaluation. An overview of this process is shown in the following illustration.

Determine Internal Distribution. Distribution is determined and noted on each incoming report. Experience has proven that a logical sequence for routing data is important. Establishing an SOP stating who gets a certain report first, second, or third is essential. Flow charting may be used to describe the distribution scheme.

Log and Distribute Incoming Reports. Incoming reports are logged in the journal and distributed immediately after receipt. Reports may be received through message center channels, by courier, or by either radio or telephone. If the report is received verbally, the information is transcribed before processing. The logging and filing of incoming messages and reports provides a historical record of data transactions and allows personnel to refer to previously reported data for—



- ☐ Comparing newly reported data.
- ☐ Adjusting collection efforts.
- ☐ Evaluating the responsiveness of tasked collection agencies to produce pertinent data on time.

Determine Source or Agency Reliability. Source reliability is determined and recorded on the incoming report by the collecting unit or agency. The ASPS personnel also judge reliability based on the past performance of the reporting unit or agency and assess an overall reliability factor for each incoming report. The overall reliability factor is marked on each report and clearly distinguished from the factor assessed by the reporting agency.

The reliability of each incoming item is evaluated by a standard system using letters A to F. The overall source or agency reliability factor is signified by various degrees of confidence as shown in the following table.

Determine Credibility of Information. Credibility is designated by a number between 1 and 6 as shown on page 3-47.

To determine the combined ratings, the two aspects of evaluation, reliability and credibility, must be considered independently. The rating is expressed as a letter-number combination. For example, information received from a usually reliable source that is judged as "probably true" is

RELIABILITY OF SOURCE/AGENCY TABLE

LETTER	DEGREES OF CONFIDENCE	USE
A	Completely reliable	Only assigned under the most unusual circumstances.
B	Usually reliable	Indicates a source or agency of known integrity.
C	Fairly reliable	Indicates a source or agency that is fairly reliable.
D	Not usually reliable	Indicates a source or agency not usually reliable.
E	Unreliable	Indicates a source or agency usually unreliable.
F	Reliability cannot be judged	Assigned when there is no adequate basis for estimating the reliability of the sources.

rated as "B2". Information from the same source, but judged as "truth cannot be judged" is rated as "B6".

Evaluate Intelligence and Information Reports

The second step in the process is evaluating intelligence and information reports. All incoming reports must be examined for pertinence in terms of reliability and credibility factors. A decision is then made concerning the report's value. Event templates are a valuable aid in determining a report's value. If a report is determined not to be pertinent, it will be filed for possible future reference. Coordination with the collection manager is made to modify or clarify tasking. Pertinent information is then fused with other information in the data base.

Information is evaluated for pertinence by determining whether the information is—

CREDIBILITY OF INFORMATION TABLE

NUMBER	DEGREES OF CREDIBILITY	USE
1	Confirmed by other sources	Used when it can be stated with certainty that the information originated from two or more different sources.
2	Probably true	Used when no proof of the above can be established, and no reason exists to suspect that the reported information comes from the same source.
3	Possibly true	Used when investigation reveals that the reported facts are compatible with the previously observed behavior of the target, or if known background of a target leads to the deduction that the target might have acted as reported.
4	Doubtful	Used when reported but unconfirmed information contradicts the estimate of the development or the known behavior of a target.
5	Improbable	Used when reported information is not confirmed by available data and contradicts the experience assumed to be reliable with regard to the development of a target or issue.
6	Truth cannot be judged	Used when an investigation or a report reveals that a basis for allocating ratings 1 to 5 does not exist.

- ☐ Pertinent in regard to the enemy or to the characteristics of the battlefield area.
- ☐ Needed immediately.
- ☐ Of future value.
- ☐ Of no apparent value.
- ☐ Of value to higher, lower, or adjacent unit.

Update Files

Intelligence files are updated by fusing incoming intelligence reports with information in the data base. Fusion is accomplished by—

- ☐ Reviewing reports to determine the event, area, and enemy unit.
- ☐ Searching files for corresponding information.
- ☐ Noting the previous report number and source or agency on the new report. (When the report cannot be correlated, it is noted as a sole-source report.)

Significant data is extracted from the reports and posted to the appropriate file. Extracts from SIGINT, ESM, and collateral reports are used to update the enemy EOB and collateral SITMAP overlays. Periodically, all SITMAP overlays are compared with the all-source SITMAP. By making this comparison, the flow of movement can be observed and enemy concentrations will appear more clearly.

Once the preceding steps have been accomplished, a second level of processing is required for further file integration. This is accomplished by—

- ☐ Posting the PIR and IR number to the report if PIR and IR have been partially or totally satisfied.
- ☐ Identifying all significant information if no PIR and IR have been satisfied.
- ☐ Fusing data with known intelligence.
- ☐ Updating the all-source SITMAP.
- ☐ Comparing the collateral and EOB overlays with the all-source SITMAP.
- ☐ Reviewing event analysis matrixes.
- ☐ Identifying major enemy movements and concentrations.
- ☐ Updating event analysis matrixes.
- ☐ Considering impact of events on TAI and NAI.
- ☐ Updating OB, if necessary.

PIR and IR are answered when the information is available. Questions are answered when there is a reasonable probability (80 percent or better) that the answer at hand is correct. The PIR and IR should be answerable at this point in the intelligence process unless the requirement involves predicting enemy intentions. If intentions are required, then the process is continued to develop an estimate of enemy probable courses of action from which to predict intentions.

Estimate Enemy Probable Courses of Action

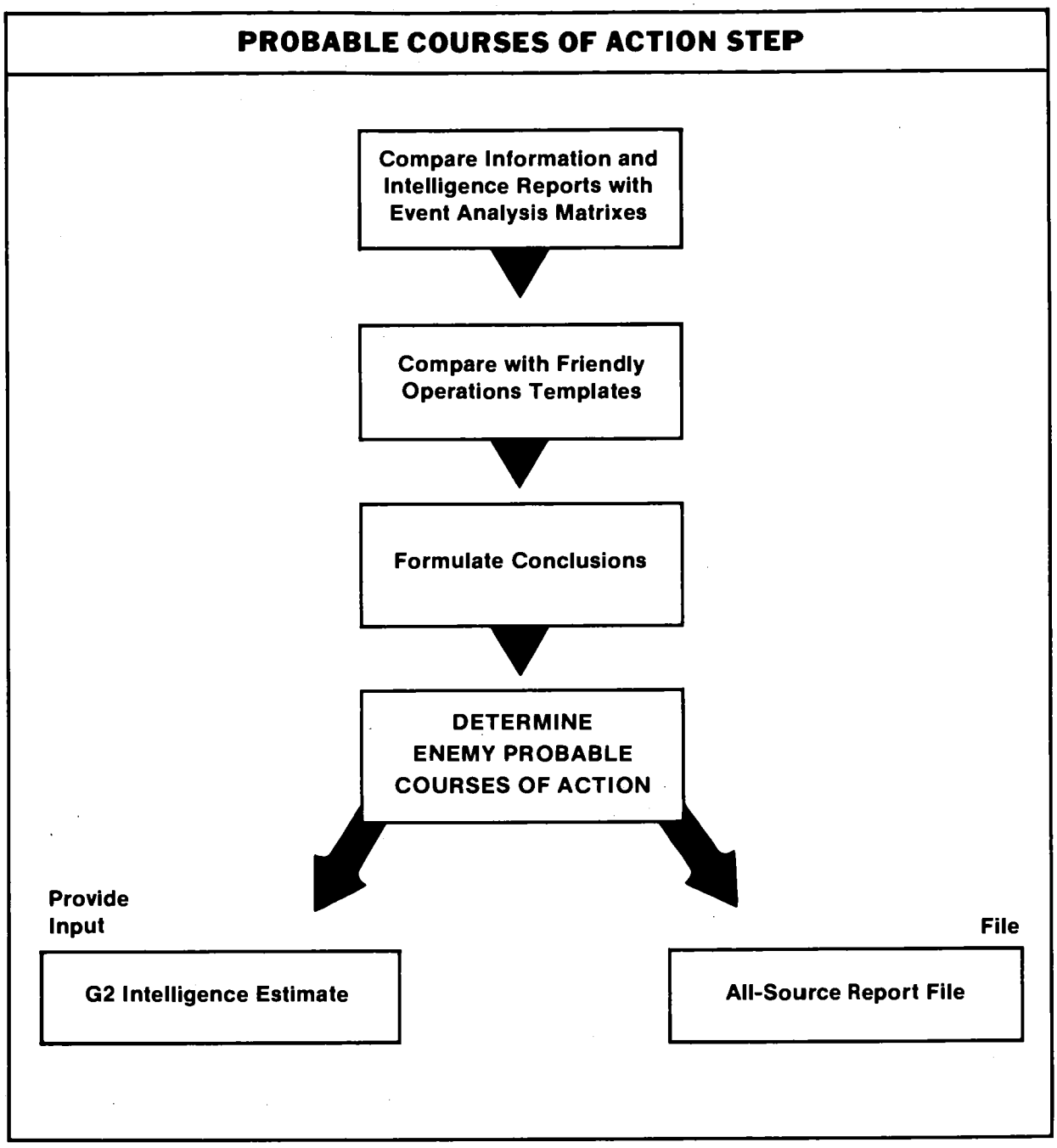
An overview of this phase of the intelligence production process is shown in the following diagram.

Compare Information and Intelligence. Comparing reports with event analysis matrixes is done by—

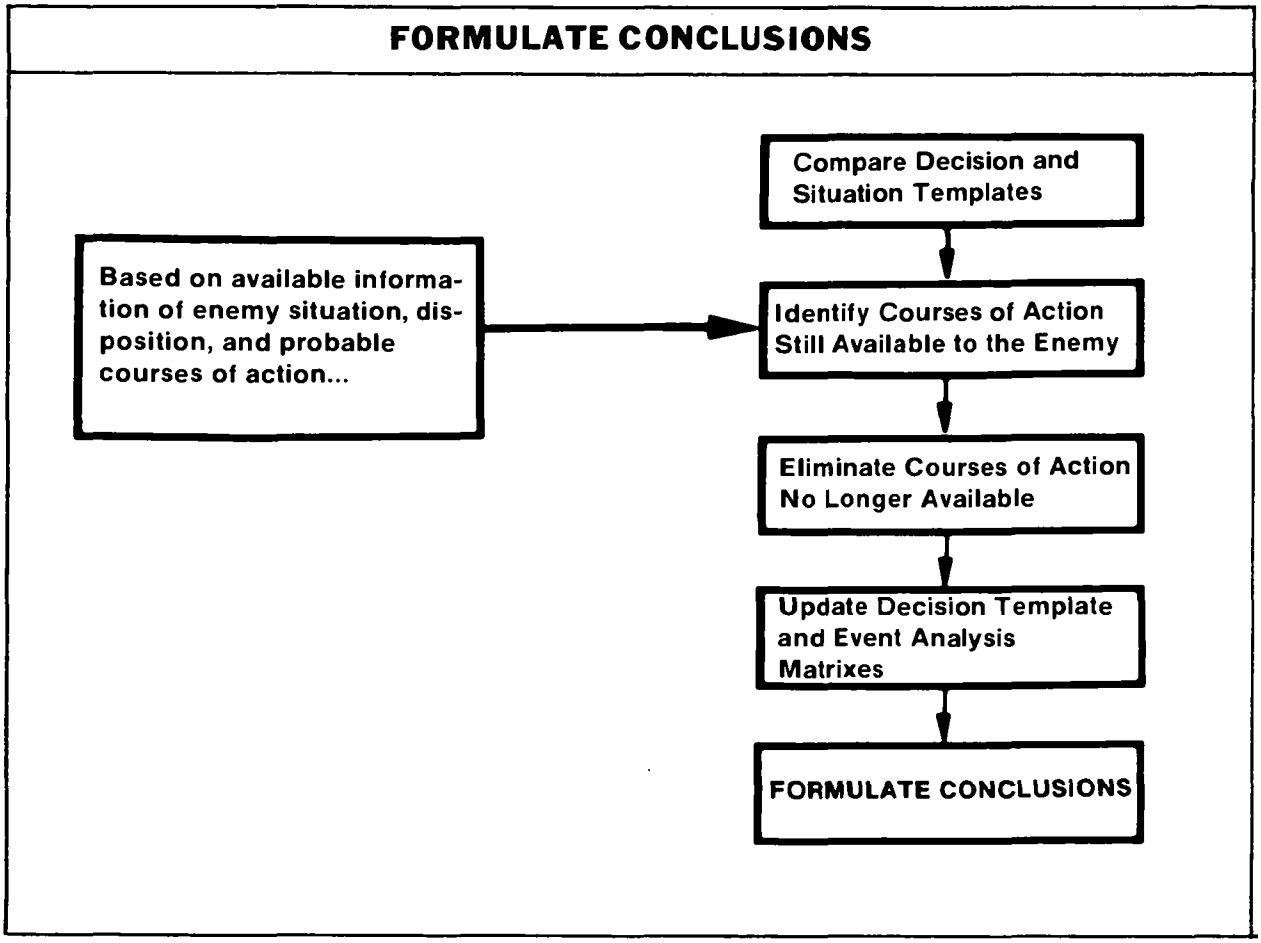
- ☐ Reviewing each report to see if it correlates with indicators in the event analysis matrix or might be a deception attempt.
- ☐ Posting usable information on decision support templates. As this information is posted, each MC is analyzed for the enemy's indicated course of action.
- ☐ Determining if events support enemy use of particular MCs.
- ☐ Identifying indicators of enemy probable courses of action.
- ☐ Considering the impact of events on TAI and NAI.

This phase provides an updated decision support template.

Formulate Conclusions. Conclusions are the last step in the interpretation of information. Conclusions are reached by logical decisions based on an analysis of available intelligence, knowledge of the battlefield area, and the enemy's situation, capabilities, and vulnerabilities. The illustration on page 3-50 provides an overview of this step.



A conclusion is arrived at through either deductive or inductive reasoning. Deductive reasoning gives meaning to certain known factors through inference—leading from the general to the specific. For instance, through radio intercept it is known that a motorized rifle regiment (MRR) is deployed and advancing along a particular avenue of approach. Based on knowledge gained through previous operations or the study of enemy doctrine, it can be deduced that this regiment has certain capabilities and vulnerabilities and will be used in a



certain way. By considering current intelligence holdings on this regiment, further deductive reasoning will provide a more specific answer. Collection agencies then can be tasked, if necessary, to confirm or refute the conclusions reached and to provide information or intelligence to the commander.

Inductive reasoning leads from specific information to a general hypothesis. For instance, over a period of time, intelligence collection systems and agencies have reported the existence of approximately eighteen 120mm mortars, eighteen 122mm howitzers, and over 100 BMPs, BTRs, and BRDMs forward of the FLOT and deployed across a 3-kilometer front. Using existing OB intelligence, doctrinal templates, and inductive reasoning, the force is identified as an MRR.

As posted intelligence reports begin to fill out decision support templates, the templates are compared with the situation templates to identify those courses left open to the enemy commander. Courses of action which, by virtue of enemy disposition, are no longer viable are eliminated. Templates are updated as necessary to reflect these changes.

Determine Enemy Probable Courses of Action. An estimate of the enemy's most probable course of action and intentions is the result of situation development. Estimating enemy intentions is accomplished by—

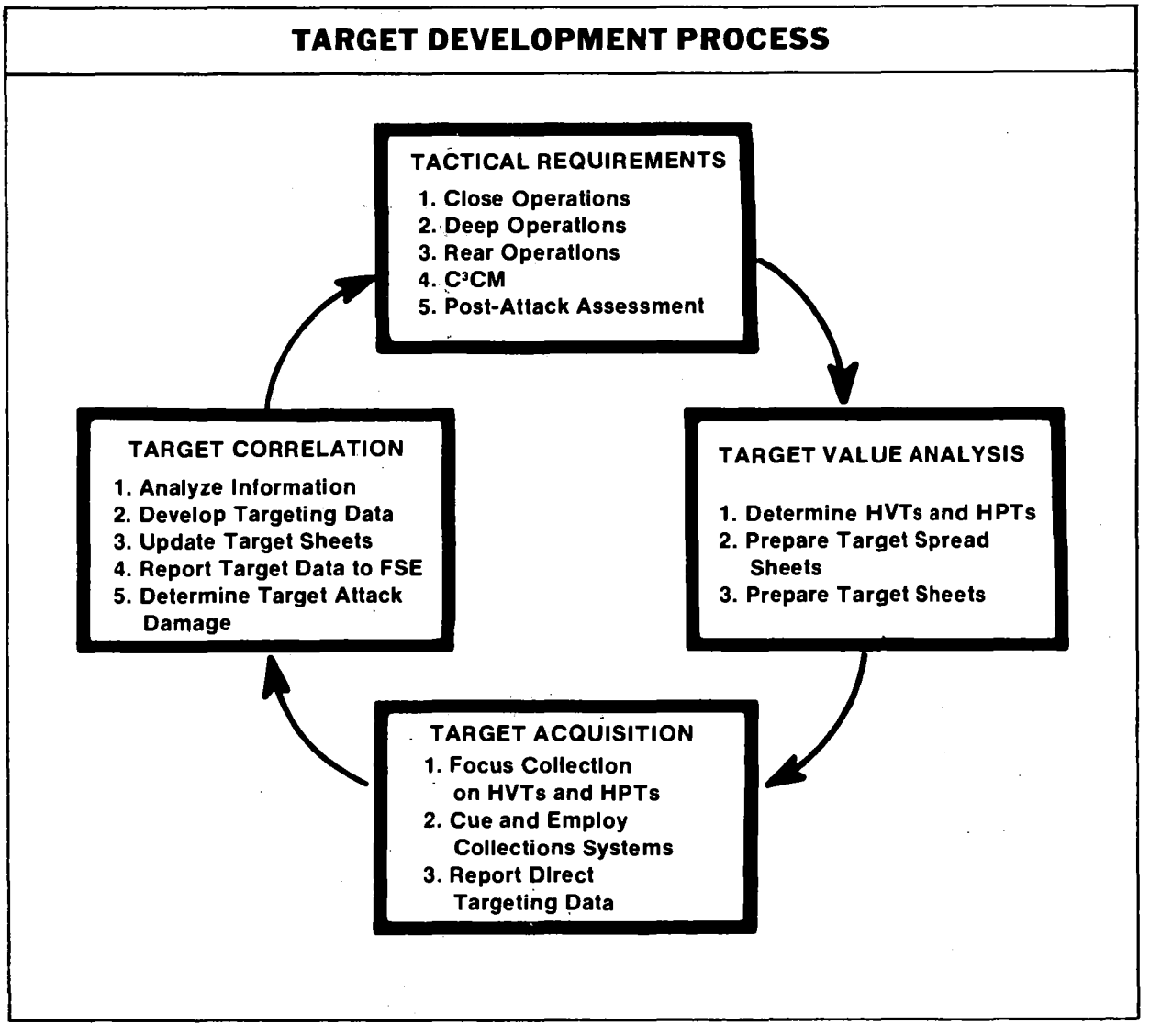
- Analyzing the current enemy situation as depicted on the decision support templates.
- Determining the enemy's most probable course of action based on those

courses of action left open to the enemy commander, the disposition and composition of the enemy force, and the friendly situation. This effort focuses on answering the PIR.

Develop Targeting Data

Target development is the process of providing targeting information to support the commander's tactical plans. Performed by the ASPS at corps and division and, to a more limited degree, by S2s at brigades and battalions it is an integral part of the all-source intelligence analysis and production process. The same collection, IPB, and analysis functions that support situation development also support target development. Where the objective of situation development is an estimate of enemy intentions, the objective of target development is to provide direct or correlated targeting data which meets the commander's target selection standards. An overview of the target development process is shown in the following illustration.

The following material addresses the IEW functions within the overall targeting process. Details on the total targeting process, to include interfaces between fire support, maneuver, and IEW are located in FC 34-118/6-34-10.



There are two objectives in the target development process. The first objective is to provide direct targeting data (combat information) to commanders for immediate fire and maneuver in close operations. The second objective is to collect and correlate information from all sources to develop targeting data for attacking second-echelon targets in deep operations.

Direct targeting data results from the immediate identification and location of targets and reporting that information directly to FSEs for attack. This normally occurs when accurate detection, identification, and location of a target is obtained from a single source and is immediately available for fire support use. An example of this would be armor targets acquired by GSR.

Correlated targeting data results from comparing or correlating information from multiple sources to accurately fix a target. Target correlation includes TVA.

TVA is a methodology for identifying HVTs and HPTs. HVTs are elements or resources of an enemy formation which the ***enemy*** commander considers to be essential to accomplishing a specific tactical objective. HVTs are determined independently of friendly capabilities to acquire and engage them. HPTs are HVTs which ***can*** be successfully acquired and engaged by a friendly force to a degree which makes the enemy formation vulnerable to exploitation. It is the successful friendly exploitation of the enemy formation which results in the tactical "PAYOFF." Using IPB templating, TVA is done before the battle so that during the battle the commander can quickly select and attack specific targets to manipulate the enemy force. When faced with a numerically superior enemy force, commanders will not have enough resources to attack every target acquired. Therefore, TVA must be keyed to determining which targets out of the entire enemy array should be attacked to achieve the greatest tactical benefit for the resources expended. TVA determines—

- ☐ The critical targets.
- ☐ When these targets should be attacked.
- ☐ Where these targets should be attacked.

TVA links the effects of attacking a target directly to target behavior. TVA begins in IPB by a detailed analysis of enemy doctrine, tactics, equipment, organizations, and expected behavior. Information derived is then used to project how, in each tactical formation, the enemy will respond when confronted with different tactical situations. Activities, behavior, equipment, and elements of the selected enemy force which are critical to successful operation in each situation are identified. An example of this is the engineer company in an MRR during a march to contact. When the MRR is faced with making a river crossing, the engineer company's location within the march formation changes. Other preparatory activities also must take place in order for the river crossing to succeed. Through TVA, a listing of actions and elements are developed that would prevent the MRR from conducting a river crossing. Preventing the river crossing may accomplish the desired effect by disrupting, delaying, or blocking the MRR based on the commander's tactical plan. In-depth TVA provides a means of determining which targets should be attacked for the greatest tactical benefit in a given situation. These targets are identified as HPTs.

When conducting TVA, the situational value of a target is a significant factor. As the distance from the FLOT increases, the value of combat forces decreases with respect to CSS forces and facilities. For example, at the FLOT, a tank battalion is a significant threat and is a very important target to the maneuver battalion commander. However, 10 kilometers forward of the FLOT, that tank battalion is not as important to the success of the enemy's immediate mission as an ammunition supply point (ASP) or a fuel dump. Recognition of this situational value element is important in TVA.

TVA tools are an effective means of functionally applying TVA and include target spread sheets and target sheets. These tools should be prepared in conjunction with the IPB effort. Target spread sheets are a means of describing and identifying targets in specific tactical situations at various

echelons of Soviet-type forces. Target sheets support spread sheets and list the critical elements of various target groups which, when attacked, will restrict options or capabilities. Both of these products are classified because of the nature of the information depicted. Once completed, these sheets are used by the G2, G3, and FSE as shown in the following chart.

SPREAD SHEET USES	
G2	**G3/FSE/EWS**
1. Focus intelligence collection assets. 2. Determine target development needs. 3. Recommend target priorities to G3 and commander.	1. Develop target priorities for the commander. 2. Development methods of attack. 3. Establish priority for attack. 4. Develop fire support plans. 5. Develop ECM plans.

Currently, target spread sheets have been prepared for use in Europe or against Soviet/Warsaw Pact-type forces in any mid- to high-intensity environment. Target spread sheets normally used are shown in the following matrix.

Each echelon of command should have and use target spread sheets and target sheets that apply to the enemy forces that command will face. These sheets are prepared and maintained by the ASPS.

SPREAD SHEETS

TACTICAL SITUATION	ECHELON OF COMMAND			
	REGIMENT	DIVISION	ARMY	FRONT
Movement to Contact	X	X		
Meeting Engagement	X			
Attack Against a Defending Enemy To Seize Subsequent Objective	X	X	X	X
Forced River Crossings		X		
Assault Crossing from the March	X	X		
Hasty Defense	X	X		
Prepared Defense		X	X	
Withdrawal	X	X	X	

During TVA and preparation of the target spread sheets, potential targets are grouped into 13 sets. These sets are shown in the following illustration.

TARGET SETS

1. Command, control, and communications.
2. Fire support.
3. Maneuver.
4. ADA.
5. Engineer.
6. Reconnaissance, surveillance and target acquisition (RSTA).
7. Radioelectronic combat (REC).
8. Nuclear/chemical.
9. Class III (petroleum, oils, and lubricants (POL)).
10. Class V (ammunition).
11. Class IX (maintenance).
12. Lift (surface transport/ helicopters).
13. LOC.

Once an analysis of enemy doctrine is completed, a target spread sheet is prepared for each specific tactical situation and level of command. A sample target spread sheet is shown in the following illustration. For a detailed description of target spread sheets, refer to FC 6-20-10.

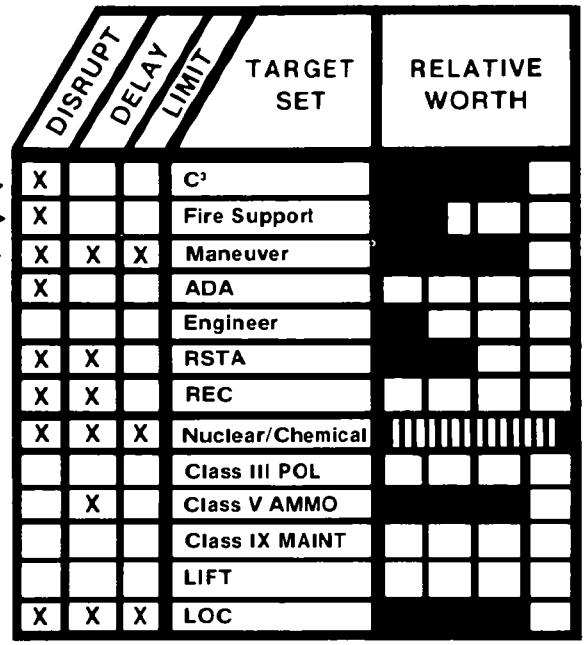
The target value matrix is divided into five columns. The first three columns describe the effect desired from attacking the target. The Xs in the columns identify which effects can be achieved in a particular situation against the size of formation for which the sheet is being prepared.

The TARGET SET column lists the 13 target sets identified previously. The RELATIVE WORTH column depicts the worth of attacking one target set with respect to the other target sets on the sheet. The subdivisions in the column are not scaled and should not be interpreted as absolute values. This column allows a rapid identification of the priority different target sets should have when resources for attack are scarce.

For target sets assigned a RELATIVE WORTH, brief statements describing the rationale for attacking each set are placed, in columnar form, to the right of the target value matrix. Specific HVTs for each target set assigned a relative worth are also listed, in columnar form, to the right of the appropriate attack rationale statement. Specific HVT listings will also contain the number of the appropriate target sheet describing each HVT for easy reference. For example, in the river crossing scenario, the engineer target set may be assessed as critical with an attack rationale statement to the effect "Halt or impede preparation of crossing site and execution of crossing." A specific HVT in this case might be the ferry crossing site with reference to a target sheet number for that HVT, for example, ***Ferry Crossing Site*** (75)."

The target value matrix also contains information on enemy doctrine. This includes likely formations and distances (doctrinal template), objectives of the force, and likely enemy courses of action if the attacks on this force are successful.

SAMPLE TARGET SPREAD SHEET (EXTRACT)



Contribution in this situation to disrupt/delay unit responses.

The nuclear/chemical target set is high payoff at division and higher levels regardless of the situation. Its contribution varies too greatly to be predictable, thus, the different graphical treatment.

Relative value of attack in this situation.

DESIRED EFFECT

	THREAT IS ATTACKING	THREAT IS DEFENDING
DISRUPT	Preclude the efficient interaction of combat and supporting systems.	Same.
DELAY	Alter arrival time of the force outside planned/predicted movement schedule.	Slow defensive preparation and/or delay reinforcement.
LIMIT	Cause the force to shift to another avenue of approach.	Isolate the defender.

NOTE: Actual target spread sheets will also contain information on the size of forces, tactical situation, specific HVTs, and doctrinal templates.

A target sheet is prepared for each potential HVT. The target sheet is numbered for references, identifies the target, and provides information on the size, doctrinal location, vulnerability, signature (visual and electronic), and probable impact of the loss of the target on the enemy's operatic A sample target sheet is provided below.

SAMPLE TARGET SHEET

TARGET CATEGORY: Engineer

HIGH VALUE TARGET: TGT 75. Ferry crossing site.

FUNCTION: Provide rapid crossing of water obstacles for tanks and other nonamphibious systems.

DESCRIPTION:

— TGT radius - point target.

— Posture - exposed on water surface FEBA distance.

COMPOSITION: Vehicles normally 2 ferries or rafts (if river over 300m wide may be as many as 5)

PERSONNEL:

SIGNATURE:

Visual - see graphic.

Electronic -

Other -

DEGRADATION:

— Nonamphibious forces must find alternate means to cross.

— Force that secured bridgehead is not reinforced.

When completed, TVA results in a list of high payoff targets for each enemy echelon of command and tactical situation. These lists are used jointly by the operations, intelligence, and fire support staffs to develop a high payoff target matrix. A sample high payoff target matrix is provided in the following illustration.

An approved high payoff target matrix can then be used to further refine attack criteria and attack guidance as to—

- ☐ What targets are to be attacked (in order of priority).
- ☐ When they are to be attacked.
- ☐ Why they are to be attacked.
- ☐ What are the conditions for success and failure.

S&T intelligence target lists must also be considered in target development. These lists can be used by fire support and operations staffs to disrupt, destroy, or capture facilities, depots, or critical materials which are important to the sustainment of enemy combat operations. These lists also may contain key enemy logisticians, industrialists, scientists, engineers, laboratory technicians, or specific documents.

S&T intelligence targets are categorized and listed by priority and reflect the target's criticality to current and planned operations:

- ☐ ***Priority I*** - highly critical to the outcome of the campaign and are probably perishable.
- ☐ ***Priority II*** - highly critical to outcome of the battle and are probably perishable.
- ☐ ***Priority III*** - significant, not perishable.
- ☐ ***Priority IV*** - desirable, not perishable.

Targeting data is developed for those targets that must be attacked to support the commander's tactical plan. Selected future targets are identified by the G3 as early as possible. This permits the detection, location, and tracking of these targets as they

SAMPLE HIGH-PAYOFF TARGET MATRIX

Priority	Target Set	Target Sheet Number	Description
1.	8 (TS)	77, 79	Nuclear Depot
2.	1 (TS)	29, 34	Division, Army Main CP
3.	2 (TS)	5	Division Artillery Command Btry
4.	2	1, 2, 18	Arty Bn FDC, COP, FA Btry
5.	1	25, 30	Regimental Main CP, Div Fwd CP
6.	3	51, 50, 46, 48	Bn Assy Area, March Column, MR/TK Co
7.	4, 7	63, 64, 91, 92	AD EW Site, Radio/ Radar Intcp Sites
8.	9	115, 116	Regiment/Division POL Points
9.	10	120, 121	Division/Army Ammo Depots

NOTE:
1. List may have any number of target priorities.
2. This list is jointly developed by G2/G3/FSE.

enter the command's battlefield area. This facilitates early target development which allows attack of targets at the optimum time and distance from the FLOT.

Collection of information for target and situation development normally occurs simultaneously. The collection manager establishes separate collection missions when priorities are sufficiently high and planned collection missions will not provide the specific information desired. Information to support target development is acquired by the same resources which collect for situation development and is divided into the same categories (movers, emitters, shooters, and sitters). Information collected for targeting purposes requires a greater location accuracy than that collected for answering PIR and IR. When determining reporting requirements to support target development, the collection manager must ensure that the specific detail needed is stated in the collection requirement. Reporting requirements must include:

- ☐ Target location accuracy required to include the sensor's target location error if applicable.
- ☐ Time target was last observed at the reported location.
- ☐ Target description.

The time required to process collected information must be as short as possible to ensure target data can be developed and reported in minimum time. The objective is to enable attack of the target while it is still where it was detected. This means that targeting data must be reported as expeditiously as possible.

Targeting data must be reported in time for decisions to be made and fire control

procedures to be completed before a target leaves a desired attack area. Quick fire channels are established between the G2 and G3 for use in reporting targets as they meet pre-established criteria.

Postattack assessment is performed by the ASPS as part of the processing function to determine the effects of deep attacks against the enemy's follow-on and supporting echelons. Damage reports and other information used to assess the effectiveness of the attacks are handled in the same way other reports are handled. The reports are evaluated for reliability and credibility, logged in, distributed, and used to update intelligence files.

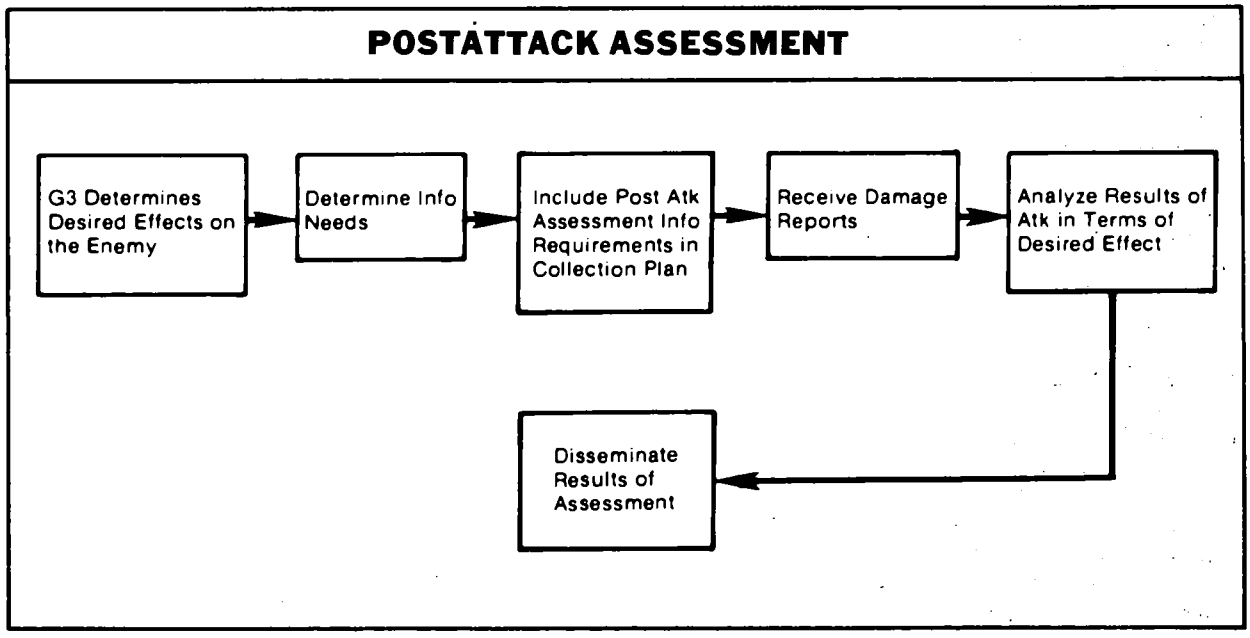
The corps or division G3 establishes the planned time and desired effects of an attack. After the attack, it is then determined, through analysis, if the criteria established by the G3 have been satisfied. Satisfaction of the attack criteria is determined by deciding whether or not the desired damage was done to the enemy. For example, the attack was to have caused an enemy unit to be delayed for eight hours; or, the intent of the attack was to force the enemy to follow a particular route. Once it is known what the attack was supposed to accomplish, its impact on the enemy force can be assessed, based on the enemy's reaction.

The postattack assessment process is shown in the following illustration.

Monitor Collection Plan

ASPS personnel constantly monitor the collection plan to provide immediate responses to collection requirements and recommend adjustments to the collection plan to meet ASPS needs. To fulfill PIR, IR, and TAI information needs, the collection plan must ensure that the required information is collected to answer the critical questions asked by the commander. The ASPS monitors the collection plan and identifies gaps by—

- ☐ Reviewing template files and the TAI overlays.
- ☐ Determining if TAI information needs match PIR and IR.
- ☐ Comparing PIR and IR to the all-source SITMAP and the event analysis matrixes.
- ☐ Determining the satisfaction of PIR, IR, and event indicators.
- ☐ Identifying, if necessary, additional information needed to fulfill TAI needs and the commander's targeting guidance.
- ☐ Informing the CM&D section of additional collection needs.



Once gaps are recognized, appropriate orders and requests are issued by the CM&D section to eliminate unproductive coverage and focus on updated collection requirements. The CM&D section is notified immediately of a gap in intelligence holdings.

Produce Intelligence Reports

Intelligence reports are produced by the ASPS to satisfy situation and target development requirements. Reports are generated based on information developed through IPB, extracted from incoming reports, or developed through all-source analysis. The production process focuses on identifying reportable information and preparing and transmitting the report to the necessary units or agencies. Reports are prepared after—

- ☐ Reviewing the decision support template and PIR and IR file.
- ☐ Reviewing the estimate of the enemy's most probable courses of action.
- ☐ Identifying enemy events which satisfy PIR and IR.
- ☐ Identifying enemy intentions supported by actual events.

A distribution planning file is used to control the reporting of intelligence. This is a list or matrix that provides a ready reference for determining the distribution of each report. The file is used in conjunction with the SOP, which stipulates report formats for each report. If an item of information does not fit within the established reporting criteria, an intelligence spot report is transmitted.

Reporting the enemy's intended or actual use of NBC weapons or the location of these weapons is especially critical. If it is determined that the enemy has or intends to initiate an NBC attack this information must be reported to higher, lower, and adjacent commands by the fastest means, with the highest message precedence. Initial reports are sent using a FLASH message precedence. Subsequent reports are transmitted with an immediate message precedence.

The locations of enemy NBC weapons are reported to the G3 or FSE by the fastest means possible. Normally the FAIO will assist in expediting targeting data of this nature. Unit SOP must provide explicit instructions for reporting enemy NBC intelligence.

DISSEMINATION

The final function supporting situation and target development is dissemination. Intelligence and combat information are of little value if not delivered when and where needed. Failure in this respect defeats a thorough and successful collection and processing effort. Since most intelligence and all combat information are time sensitive, they must be disseminated to commanders and others who need it, when they need it, and in a form they can use.

The free, timely exchange of intelligence and combat information is critical to success on the battlefield. Dissemination is driven by battlefield events. Fast-moving battles dictate the need for transmitting information quickly. Electrical message, data link, secure voice radio, and courier are the primary means of dissemination. Fragmentary reports transmitted quickly carry the bulk of intelligence and are preferred over schedule-driven, standardized reports. Although the methods and means used to disseminate intelligence and combat information are similar, there are significant differences that must be considered.

Timely dissemination of intelligence enables commanders to make decisions with confidence. It also provides knowledge in light of new information which may be processed. Intelligence is used in much the same way at all echelons. The means of dissemination are likewise similar at all levels but volume, distribution, and frequency vary. Intelligence is disseminated within the producing headquarters and to the next higher, next lower, and adjacent units. Dissemination to lower and adjacent units is more difficult and yet more important, because—

- ☐ The intelligence picture at lower echelons changes more rapidly.

- ☐ The requirement for greater detail may result in delay.
- ☐ The specialized intelligence produced only at higher echelons may have significant bearing on the operations of lower echelons.

Combat information and targeting data are the mainstay for brigade and battalion commanders and fire support units. Commanders use this data for immediate action against the enemy. Any element that obtains combat information must disseminate it by the fastest, most direct means available. This is achieved by entering the appropriate intelligence net or, as appropriate, the command net. When direct communications are not possible, the information is passed through available communications to a relaying headquarters. Combat information also is reported through intelligence channels for processing and dissemination. The FAIO assists in disseminating targeting data to the appropriate FSE. Intelligence, combat information, and targeting data are disseminated based on established requirements. Each unit must establish a system to differentiate between priorities so that only its most critical information is disseminated immediately.

REQUIREMENTS

The principal requirements for dissemination are timeliness, usability of form, pertinence, and security.

Intelligence and combat information are disseminated in time to permit formulation of plans and initiation of action using that data as a basis. Certain items of information, such as a report of an impending counterattack, must be disseminated immediately to permit maximum reaction time. The immediate significance of such combat information is obvious and thus does not require much evaluation before transmitting. After transmitting, it is analyzed for further significance. The resulting intelligence is disseminated as rapidly as possible. Timeliness in the dissemination of intelligence is affected by the dissemination means employed.

Intelligence must be disseminated in a form which will permit its ready use. The form varies according to the nature and location of the prospective user, the urgency and nature of the intelligence, and available means of dissemination. Dissemination to the commander, the unit staff, and subordinate units located near the CP is accomplished through personal briefing using the SITMAP. Combat information and intelligence should be disseminated in the form of brief messages to permit prompt understanding and use. Information which can best be shown graphically should, consistent with other requirements, be disseminated in the form of overlays, so that it can be readily applied to the SITMAP of receiving units. Written intelligence estimates, intelligence annexes, and intelligence reports are effective dissemination tools when the requirement is for general dissemination of a large amount of information.

Caution must be exercised to ensure that all intelligence is disseminated to all units and agencies which have a need for it. In this sense, broad dissemination is preferable to dissemination which is so selective that units may fail to receive the intelligence they need. However, dissemination should not result in units frequently receiving irrelevant intelligence which they cannot use or large amounts of information that ties up their communications channels. This is especially valid in the case of dissemination to brigades and battalions, because of their limited capabilities for processing and storage. Generally, dissemination to subordinates is based on the pertinence of the intelligence to the unit concerned. Intelligence is disseminated to adjacent units on the same basis without going through the chain of command. Conversely, virtually all intelligence should be disseminated upward.

Changes in the tactical situation may cause an item of intelligence which was once thought to be unnecessary, to become pertinent.

The enemy's awareness that friendly forces have certain intelligence concerning their situation may cause them either to alter their actions so that the intelligence is no longer valid or to strengthen their security effort. This makes subsequent collection

of information by friendly agencies difficult. Accordingly, dissemination is accomplished with adequate transmission security. Classified messages which are transmitted by a means susceptible to enemy interception are normally encrypted.

Dissemination officers should be aware that certain types of SCI may not, by national-level mandate, be decompartmented or sanitized for collateral level distribution. Any requirement to decompartment or sanitize SCI must be coordinated with the command SSO. Any decision by the command SSO or the senior intelligence officer to disseminate SCI in contravention of national-level directives as a result of a time-sensitive combat requirement must be reported to the SSO at the next higher level of command.

MEANS

There are various means available for the dissemination of combat information and intelligence. Combat information is transmitted by the most direct means. Normally, it flows from the collector directly to the user by voice or message transmissions. Intelligence may be disseminated by—

- Any available communication means.
- Direct contact in the form of conferences, briefings, and liaison visits.
- Issuance of intelligence documents such as intelligence annexes, INTSUMs, and periodic intelligence reports (PERINTREPs).

Dissemination within a headquarters is usually made by personal contact, verbal reports, briefings, and by distribution of intelligence estimates and written reports.

Dissemination to higher, lower, and adjacent units is made by reports, summaries, estimates, and similar documents. In most cases, reports as formulated in Appendix G or in Joint Interoperability of Tactical Command and Control Systems (JINTACCS) formats are used. Selecting the communication means for such reports depends on the urgency of the information, the types of communications available, and security requirements.

With the exception of combat information, the selection of communication means is usually the function of the CM&D section. It involves determining the operational status of each communications system and the existence and extent of message backlogs, by precedence category, for each system.

Selection

Selecting the most suitable means to be used for dissemination depends principally upon the nature and urgency of the intelligence and the means available. When wide dissemination of a comparatively large amount of intelligence is required, it is usually disseminated by the issuance of appropriate intelligence documents. As examples, during the planning phase of an offensive operation, written intelligence estimates and intelligence annexes to operations plans are used. INTSUM, PERINTREP, and periodic intelligence summary (PERINTSUM) are also used similarly during the current phase. Electrical communication means are effective for the dissemination of intelligence messages. However, such dissemination may be subject to delay because of requirements for transmission of other messages of higher priority. The imposition of radio silence requires that messages be delivered by visual means or by messenger or courier. Graphic materials such as sketches, overlays, and reports can be disseminated by means of facsimile equipment. Availability of automatic data processing (ADP) equipment will permit rapid dissemination of urgent items. Close liaison with the C-E officer is necessary to keep informed on the availability of communication means. Frequent intelligence liaison visits between units, particularly from higher to lower units, should be emphasized.

Products

The products used to disseminate combat information and intelligence depend upon their intended use. Command SOP dictates what products to use and when to use them.

Spot reports are one-time reports used by all echelons to transmit intelligence or information of immediate value. Since

information or intelligence may have an immediate and significant impact on current planning and operations, speed of transmission is essential. The spot report is afforded the most expeditious means of transmission consistent with required security. There is no prescribed format for the spot report; however, it should provide information on size, activity, location, unit, time, and equipment (the SALUTE formula).

The intelligence report (INTREP) is a standarized report which is disseminated on a required basis. An INTREP is prepared when facts influencing the enemy capabilities have been observed or when a change in enemy capabilities has taken place. The INTREP is passed to higher, lower, and adjacent units at the discretion of the commander producing the report. It is dispatched as quickly as possible following receipt of the information and is sent by the most expeditious means available. There is no prescribed format for the INTREP except that the acronym "INTREP" will be the first item to appear in the report. However, when involved in joint service operations, originators of INTREPs will use the format contained in Chapter V, JCS Publication 12. Time permitting, the INTREP includes the originating office's interpretation of the information or intelligence being reported.

The INTSUM contains a brief summary of information of intelligence interest covering a period of time designated by the commander. The INTSUM provides a summary of the enemy situation in forward and rear areas, enemy operations and capabilities, and weather and terrain characteristics. The INTSUM is an aid in assessing the current situation and updates other intelligence reports. Negative information may be included in the INTSUM, but unnecessary information is excluded. The INTSUM reflects interpretations and conclusions of enemy capabilities and probable courses of action.

The INTSUM is normally prepared at brigade and higher echelons and is disseminated to higher, lower, and adjacent units. It has no prescribed format except that "INTSUM" will be the first item of the report. However, when involved in joint service operations, originators of INTSUMs will use the format contained in Chapter V, JCS Publication 12. Nonessential detail should be excluded from the INTSUM, but information concerning the issuing unit, DTG of issue, brief discussion of capabilities and vulnerabilities, and conclusions should always be included.

The supplementary intelligence report (SUPINTREP) is a NATO standarized report form used for more comprehensive reviews concerning information on one or several specific intelligence targets. It may also contain selected intelligence data collected over an extended period of time and may include items contained in the INTREP or INTSUM. The nature and content of data contained in the SUPINTREP dictate the specific dissemination. At the commander's discretion, the SUPINTREP is passed to higher, lower, or adjacent units. It is normally produced on special request or in support of a particular operation, and is dispatched by the most suitable means available.

The PERINTREP is a summary of the intellignce situation for a specified period, normally 24 hours, in a tactical situation. The PERINTREP is a means of disseminating detailed information and intelligence. It covers the enemy situation, operations capabilities and vulnerabilities, characteristics of the area of operations, and CI. Other intelligence documents such as S&T intelligence summaries, intellience interrogation reports, translations of captured documents, and weather and climatic summaries may be disseminated as annexes to the PERINTREP. The PERINTREP is concise, but complete, and makes maximum use of sketches, overlays, and annotated maps. The use of abbreviations and unnecessary references to map coordinates is avoided.

The PERINTREP normally is prepared at corps and higher echelons. Corps may dispense with the PERINTREP if the situation does not permit timely dissemination. Dissemination is made by the most suitable means, usually by liaison officers or messengers to staff, adjacent units, and to the

subordinate and higher headquarters at the next two higher and lower echelons. The PERINTREP should be disseminated in time for use in daily planning. In joint service operations, the PERINTREP is replaced by the PERINTSUM. The format for the PERINTSUM is contained in Chapter V, JCS Publication 12.

The weekly intelligence summary generally follows the format of a PERINTREP (or the PERINTSUM in joint service operations). It serves to highlight trends that are useful in planning future operations and in processing current information. This report normally is prepared at EAC.

Imagery analysis reports disseminate IMINT. The basic types of imagery analysis reports are the reconnaissance exploitation report, initial programed interpretation report, and supplemental programed interpretation report. These reports are prepared and disseminated by the imagery analysis section in the MI battalion (AE). During joint service operations, the applicable portion of JCS Publication 12 will be used.

Intelligence interrogation and translation reports summarize the results of interrogations of EPWs, civilian detainee, or refugees, and translations or summaries of enemy documents. Information of immediate value is disseminated in spot reports. Other information is disseminated in the most suitable form for the users. At corps and higher echelons, information gotten from interrogation and translation reports is included in the PERINTREP (or the PERINTSUM in joint service operations).

Information on enemy bombing, shelling, or mortaring activity is initially disseminated by means of a bombing report, shelling report, or mortaring report (BOMREP, SHELREP, or MORTREP), as appropriate. Submission is a responsibility of the affected unit. SHELREPs and MORTREPs are provided to the affected unit's fire support officer (FSO) for input to the counterfire element of the force artillery TOC. Reports are rendered as normal messages and are transmitted by the fastest means available. Each transmission is preceded by "SHELREP" in the case of enemy artillery or by the code word "BOMREP" in the case of an enemy air attack. The text of the message is transmitted in the clear except that the current call sign of the unit of origin will be used rather than unit identification. Also, the position of the observer will be encrypted if it discloses the location of a headquarters or an important observation post.

Initial reports and data of enemy or unidentified nuclear detonations and biological or chemical attacks are disseminated from the source, through designated headquarters to the highest headquarters in the area. Reporting is by flash precedence. Initial and follow-up reports are evaluated at each headquarters and the results are appropriately disseminated.

Warning of expected contamination from a nuclear burst or biological or chemical attack is disseminated by the first headquarters capable of determining such information.

Weather forecasts are a prediction of the weather conditions at a point, along a route, or within an area for a specified period. The accuracy and reliability of weather forecasts depend upon such factors as characteristics of the area, available weather data, reliability of weather communication facilities, and length of forecast periods. Weather forecasts use encoded graphics or plain language formats. Weather forecasts for use by troop units are usually in plain text formats. The three types of weather forecasts are—

- A short period forecast, which is any forecast (to include weather warnings) covering up to 72 hours.
- An extended period forecast which covers a period of between 3 and 5 days.
- A long period forecast which covers a period of 5 days or longer.

Besides the forecasts mentioned above, an outlook may also be given as an extension to the basic weather forecast (for example, a 48-hour outlook beyond a 24-hour weather forecast). See FM 34-81/AFM 105-4 for further information.

Because of the changing nature of weather forecasts, especially short period forecasts, timeliness is a critical factor in their dissemination. Weather forecasts normally are transmitted by electrical means. The intelligence officer makes provisions for timely dissemination of severe weather warnings to enable units to take necessary preventive action. Severe weather warnings usually cover tornadoes, thunderstorms, dust and sand storms, extremely heavy precipitation, freezing temperatures, winds above specified speeds, and freezing precipitation. Warnings are issued by the supporting weather team, as required. Flood warnings are the responsibility of the unit engineer. Severe weather warnings are normally disseminated as spot reports.

Current weather reports contain information on existing weather conditions or specific weather elements. They may be verbal, written, or graphic representations provided by Army aviators, field artillery target acquisition units, field artillery meteorological sections, or supporting USAF AWS elements. Other units furnish current weather reports as directed. Normally these reports are disseminated directly to the user by the collection agency.

Summaries of weather and climate are used as a basis for other estimates and plans. They are usually prepared by the supporting weather team at the request of the intelligence officer and disseminated in intelligence documents such as the analysis of the battlefield area, intelligence estimates, and PERINTREPs. Weather summaries are used in analyzing the effects on recent operations and in estimating the effects of weather on future operations. They are required for engineer forecasts of streamflow, conditions of ground, and trafficability. Weather summaries have no prescribed format or content. The content of a weather summary is determined by the requester based on intended use.

Climatic summaries give statistical data in terms of averages, extremes, and frequencies of occurrence for a specified period of time such as a year, season, or month, at a given point, along a route, or within an area. Climatic summaries are compiled from historical records of weather observations over long periods. Format or content are not prescribed.

Climatic studies are the compilation of the climatic data (climatic summary) and the analysis and interpretation of the data in light of its possible effects on military operations. Climatic studies usually are prepared at corps and higher headquarters. Detailed climatic studies for areas of the world are included in the National Intelligence Survey (NIS). The supporting weather team prepares climatic studies to meet the particular requirements of the command. Climatic studies are disseminated on the same basis as weather and climatic summaries.

S&T intelligence bulletins and summaries are prepared at corps and higher headquarters to disseminate the results of an examination and exploitation of enemy materiel. Bulletins usually deal with individual items, while summaries are broader in scope to include such areas as scientific implications and logistics. They are disseminated through command or intelligence channels, depending upon the scope and nature of the contents. The current NATO standardized nomenclature for Soviet Bloc army weapons and equipment described in FM 100-2-3 is used in S&T intelligence reports.

Engineer terrain teams provide terrain reports and specialized engineer reports in support of the G2.

OB books contain lists, histories, code names, and other data concerning foreign units and biographical data on foreign military personalities. OB handbooks contain data concerning the political structure, military system and organization, equipment, and tactical doctrine of foreign nations. OB books and handbooks are usually prepared by DA and theater headquarters. EAC may issue supplements to keep these documents current.

AUTOMATED INTELLIGENCE SUPPORT

The introduction of computers and dedicated intelligence communications will enable the G2 or S2 to collect, process,

analyze, and produce more pertinent, reliable data, in a much shorter time than with current manual systems.

Currently, almost all analysis is done in a manual mode. The analytic functions described in this chapter are performed by the analyst with no assistance from automation. This process is time-consuming, cumbersome, and personnel-dependent. Automated assistance is presently being incorporated into many newly fielded systems. Systems still in engineering and advanced development include automated assistance.

Emphasis now is directed toward developing and fielding an automatic data processing system (ADPS) to enhance the analytic process. The ADPS is seen as an enhancement of the analytic process, not a replacement for the analyst. While systems presently envisioned will be capable of some degree of analysis, that will not be their primary function.

Army units around the world are presently using a variety of off-the-shelf ADPS. These systems vary considerably in application and sophistication. They all, however, afford the analyst the opportunity to develop familiarity with ADP, which will ease the transition into a fully automated system.

Throughout the Army there are Intelligence Data Handling Systems (IDHS) facilities that are the Automated Systems Activity (ASA) under INSCOM. The ASA IDHS provides the secure switchboard to connect analysts with the national intelligence systems assets. There are a number of software systems under development that use ASA as the conduit to national assets. There are also a number of complete computer supported systems being developed. We will address one software—the Modular Architecture for the Exchange of Intelligence (MAXI), and one complete system—the All Source Analysis System (ASAS).

The MAXI is a component of the Common Users Baseline for the Intelligence Community (CUBIC) software program. The CUBIC program provides an orderly and systematic approach for developing, implementing, disseminating, maintaining, and supporting common software for the IDHS and other qualified agencies or activities that use minicomputers. This system allows the analyst access to, among others, the Defense Intelligence Agency On-line System (DIAOLS), the Community On-Line System (COINS), the Advanced Imagery Requirements and Exploitation System (AIRES), the Pacific Command Data Systems Center (PDSC), the Analysts Intelligence Display and Exploitation System (AIDES), and SIGINT On-Line Intelligence System (SOLIS). MAXI gives the analyst a work file capability for—

- Storage and manipulation of information.
- Message generation, transmission, and reception.
- Analyst-to-analyst communication.
- Numerous other functions.

A complete system, the ASAS is a computer assisted, tactically deployable, modular all-source processing system capable of providing IEW and OPSEC support to light and heavy units at division, corps, and EAC. It consists of a common set of modules with each module performing a unique set of functions. All modules consist of vehicle-mounted shelters. ASAS is a self-contained, self-supporting system that consists of the six following major functional areas:

- Collection management (requirements management, mission management, asset management).
- Intelligence processing (single source analysis (MTI, fixed target indicators, HUMINT, COMINT, ELINT, COMINT and ELINT integration) and all-source processing).
- Situation development.
- Target development.
- EW support.
- OPSEC support.

ASAS has the capability of processing the intelligence data transmitted to it from its supporting units and the message traffic received by it. ASAS at present, does not have connections with the national data bases except by message traffic received by the system.

CHAPTER 4

CounterIntelligence

CI includes those intelligence activities intended to detect, evaluate, counteract, or prevent hostile intelligence collection, subversion, sabotage, terrorism, or assassination conducted by or on behalf of any persons or organizations operating to the detriment of the US Army. It includes the identification of the hostile, multidiscipline intelligence collection threat; determination of friendly vulnerabilities to that threat; and the recommendation and evaluation of security measures. CI supports OPSEC, rear operations, and tactical deception, and anti-intelligence warfare as part of those actions critical to the protection of our plans, units, and operations. This chapter describes, in general terms, the enemy intelligence threat, tasks which must be performed, and the integration of CI with the command's tactical operations. FMs 34-60 and 34-60A, provide a detailed description of specific methods and procedures for providing CI support. FM 34-62 provides detailed information on special methods and procedures for counter-SIGINT support.

SUPPORT TO OPERATIONS SECURITY

CI support to OPSEC orients on defeating or degrading an enemy's multidisciplined intelligence effort. It includes those counter-HUMINT, counter-IMINT, and counter-SIGINT measures necessary to oppose effectively the collection systems available to the enemy at the tactical, operational, and strategic levels. It also includes CI analysis performed as an integral part of the OPSEC process. In order to fully appreciate the value of OPSEC and, in turn, CI support to OPSEC, it is necessary to have a basic understanding of the enemy intelligence threat.

THREAT

Since most potential enemies of the US are trained in Soviet military doctrine, the following paragraphs are based on the Soviet doctrinal approach to intelligence.

Intelligence collection and target acquisition are the means by which Soviet ground commanders acquire information on opposing forces. Rapid success in military operations, a basic tenet of Soviet doctrine, demands that commanders have timely information on the terrain, weather, and their opponents. Their doctrine recognizes three general types of intelligence:

- Strategic intelligence is collected to ensure national safety and to provide information for conducting strategic military operations.
- Operational intelligence concerns itself with the application of theories and practices to current operations of fronts and subordinate armies.
- Tactical intelligence is considered the most important category of military intelligence for ensuring the success of tactical operations (division level and below). Tactical intelligence collection is conducted to obtain information necessary for the preparation and conduct of tactical operations—air, ground, and sea.

The Soviets have an excellent intelligence collection, analysis, and dissemination capability. This capability is organic to all echelons from front through regiment. Below regimental level, the results of reconnaissance operations are passed to regimental level or above for evaluation. The Soviet commander uses this capability to detect, locate, and, if possible, destroy enemy forces.

To the Soviets, reconnaissance is the most important element of combat support. It is defined as all measures taken to collect information on—

- Nuclear weapons and other means of mass destruction.
- Formations.
- Organization for combat.

- Intentions.
- Weather and terrain of the specific area of future operations.

The Soviets recognize that in order to make maximum use of their massed firepower and mobility, their target acquisition capabilities must be characterized by accuracy and short reaction times. Tactical reconnaissance is conducted to varying depths by specialized reconnaissance units as well as all other troop units.

The Soviets also recognize that reconnaissance operations will be met by countermeasures and deception operations. For this reason, diverse, multidiscipline collection means are employed to obtain information. The various collection means often overlap and are redundant. Reconnaissance is organized by commanders and staffs of all combat arms and services. Soviet tactical writings state that reconnaissance is effective only if it is conducted actively and continuously under all conditions and circumstances. Continuity of action, timeliness, and accuracy of information are constantly stressed. Soviet principles for reconnaissance missions are—

- Aggressiveness. Decisive actions and initiative are used by commanders and headquarters to obtain necessary information by all means available.
- Continuity. Intelligence is acquired at all times, regardless of the intensity of combat, time of day, or weather conditions.
- Timeliness. The gathering and reporting of reconnaissance information to allow sufficient time to counter enemy action is stressed.
- Reliability. Information is verified by more than one source to accurately portray the tactical situation.
- Accuracy. The exact determination of coordinates of important targets such as missile installations and nuclear storage sites is essential.

Air reconnaissance is a good source of tactical intelligence and is undertaken by aircraft of the frontal aviation. These aircraft have visual, photo, infrared, radar, and SIGINT capabilities. Reconnaissance aircraft, in general, also carry weapons and are capable of attacking ground targets of opportunity. A certain portion of reconnaissance missions are accomplished by pairs of fighter and ground attack aircraft assigned locate and attack missions. These missions are directed particularly against nuclear delivery sites.

The Soviets are credited with air reconnaissance capabilities similar to those of the West. If a high priority is assigned to a reconnaissance mission and mission analysis, targets might be engaged within 2 hours after imaging.

The Soviets have an extensive intercept capability for both radio and radar. Intercept units are moved forward just behind leading maneuver regiments. They have the capability to intercept all electronic emissions within the following distances from the FLOT:

- Target acquisition radar: about 25 kilometers.
- VHF: about 40 kilometers.
- HF ground wave: about 80 kilometers.
- HF skywave: unlimited.

These ranges are greatly extended when airborne intercept equipment is used. Information derived from the intercept of "clear" traffic is immediately evaluated and exploited. Decryption is normally very slow.

The Soviet DF capability is equivalent to that for intercept. While information from DF is evaluated quickly, it is unlikely to provide a sufficiently accurate fix on a moving, tactical target. If a nuclear strike is required, confirmation is most likely accomplished by aerial reconnaissance. At least 2 to 2-1/2 hours might elapse from initial electronic intercept before a strike is launched. Targets within artillery range, such as forward command and control facilities, are attacked within minutes after DF.

Reconnaissance in depth is carried out by specially trained personnel. Organized into teams, they operate up to 100 kilometers forward of the main force and can be expected to infiltrate deep into division, corps, and EAC rear areas. Their primary mission is to collect information concerning

nuclear weapons, units in assembly areas, moving headquarters, technology, and communication facilities. Normally, teams are equipped with long-range radios and, except in emergencies, probably report by burst transmission on a scheduled basis to minimize detection.

All combat units of the Soviet Army have organic tactical ground reconnaissance capabilities. Motorized rifle and tank divisions and regiments have reconnaissance battalions and companies equipped with tanks and scout cars, infantry fighting vehicles, and motorcycles. These units often operate up to one day's march ahead of the main body. Regiments on the march dispatch battalion-sized advance guards forward of the main body. The advance guard sends a company forward, and that company deploys a reconnaissance patrol of reinforced platoon strength. Engineer, artillery, and chemical troops all have their reconnaissance elements which are cross-attached to leading reconnaissance units in the advance. These same elements are always close to the FLOT in more static situations and continually perform reconnaissance for target acquisition and combat planning.

Front, army, and divisional artillery units have an organic target acquisition capability. Generally, these units have surveillance and weapon locating radars. They are also capable of sound ranging out to about 14 kilometers from the FLOT and flash spotting from OPs.

The intelligence derived by the Soviets from imagery and signals is not considered to be sufficient to determine the morale of troops, the level of combat effectiveness, nor intentions. To obtain this data, great emphasis is placed on aggressive patrolling. The capturing of prisoners is considered essential to tactical intelligence collection at all levels. Troop units gain information by using—

- ☐ OPs.
- ☐ Raids.
- ☐ Ambushes.
- ☐ Patrolling of designated areas.

The chart on page 4-4 shows the range of Soviet tactical reconnaissance assets in relation to the FLOT.

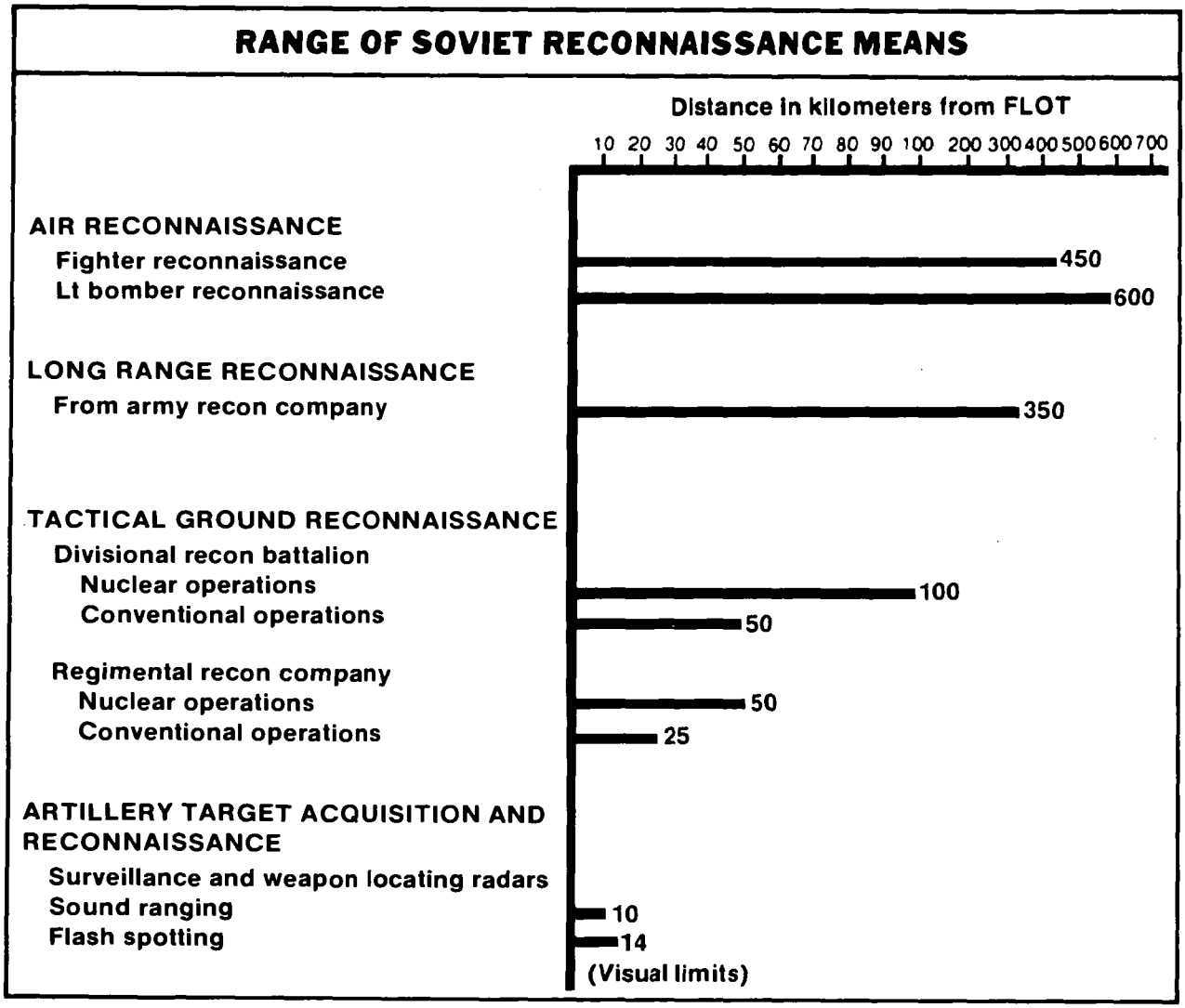
Intelligence collection threats to US forces vary according to many factors such as the depth and density of friendly forces and the weather and terrain. The chart on page 4-5 depicts a general estimate of the enemy's capability to collect against various echelons.

RESPONSE

The intelligence threat described in the preceding paragraphs means that US commanders must take specific actions to minimize the enemy's ability to collect against them. Such actions are embodied in the command's OPSEC program. This program includes the coordinated application of a variety of measures and procedures tailored to the unique requirements of each unit, mission, and situation. This requires a totally integrated effort consisting of actions in three major categories of OPSEC measures: countersurveillance, countermeasures, and deception measures.

Countersurveillance measures are those measures routinely taken to protect the true status of friendly activities and operations from enemy intelligence activities. They include measures which are integrated in daily training, such as the use of secure communications, correct electronic maintenance procedures, and camouflage and concealment. Such measures generally are required by regulations, directives, or SOP.

Countermeasures are planned, recommended, and selected to overcome specific aspects of enemy intelligence collection operations which are not countered by more routine countersurveillance. Once a friendly vulnerability is identified and determined to be a risk, a specific countermeasure is developed to preclude exploitation by the enemy. Countermeasures may include both protective and offensive actions. Protective measures include those taken to protect against hostile collection without directly attacking the collector. Offensive measures include ECM, fire, and maneuver directed against the collector. Although countermeasures are



always written into each SOP, specific countermeasures are dependent upon the situation and the mission.

Deception is all action taken to mislead the enemy into actions which are counter to his intentions. This can be done as a separate operation in support of the unit's mission or it can be used as an OPSEC measure to protect the real operation. Deception measures used as OPSEC measures are aimed more at the collector and the analyst as opposed to the enemy decision makers.

OPSEC encompasses every element of the command and requires the involvement of commanders, staffs, and troops to be effective. In fact, every soldier must take an active part in protecting the command through OPSEC. OPSEC is directed and guided by the commander, coordinated by the operations officer, supported by other staff members, and executed by the soldiers of each unit.

SOVIET COLLECTION MEANS					
ENEMY	COLLECTION AGAINST				
HUMINT	EAC	CORPS	DIV	BDE	BN
Agents	X	X	O	O	
Line Crossers	O	O	O	X	X
Recon Units		X	X	X	X
Combat Units			X	X	X
Patrols				O	X
EPW	O	O	O	X	X
SIGINT AND REC					
Radio Intcp	X	X	X	X	X
Radar Intcp	O	O	O	X	X
DF	O	O	O	X	X
Sonic			O	O	X
IMINT					
Photo	X	X	X	X	X
Infrared (near/far)	X	X	O	O	O
Radar Survl	O	O	O	X	X
Early Warning Radar	X	X	X	O	O
REMS		O	O	X	X
Night Vision Devices					X
Visual					X
SLAR	O	X	X	X	X

LEGEND X - High Threat
O - Moderate Threat
Blank - Limited or no Threat

The OPSEC program must be applied to all aspects of military operations during peace and war. Its objectives are to support our principles of war, to ensure command security, and to preserve the element of surprise. To be effective, an OPSEC program must be—

- ☐ Established by the commander.
- ☐ Emphasized at all levels of command.
- ☐ Designed for the single purpose of providing security to the command.
- ☐ Based on operational requirements.
- ☐ Aggressively implemented.
- ☐ Adaptable to changing situations.

Staff Responsibility

The G3 has staff responsibility for the command's OPSEC program in coordination with the G2 and reinforced by the OPSEC staff element. The G3—

- ☐ Manages the command's OPSEC program.
- ☐ Develops EEFI and associated indicators for each operation.
- ☐ Establishes OPSEC policy and procedures.
- ☐ Prepares OPSEC estimates, plans, and annexes.
- ☐ Reviews OPLANs and similar documents to ensure adherence to OPSEC policies and procedures.
- ☐ Develops friendly force profiles with the assistance of other elements of the command.
- ☐ Evaluates operational risks.
- ☐ Selects OPSEC measures.
- ☐ Directs OPSEC evaluations.

The G2 has staff responsibility for CI and performs the CI staff functions needed to support the OPSEC program. The G2—

- ☐ Coordinates the collection and processing of intelligence to support the OPSEC program.
- ☐ Recommends EEFI to the G3.
- ☐ Evaluates hostile intelligence, sabotage, subversion, and terrorism capabilities.
- ☐ Has staff responsibility for defensive source nets and tactical agent operations (when approved by EAC).
- ☐ Performs staff supervision of all CI activities of the command.

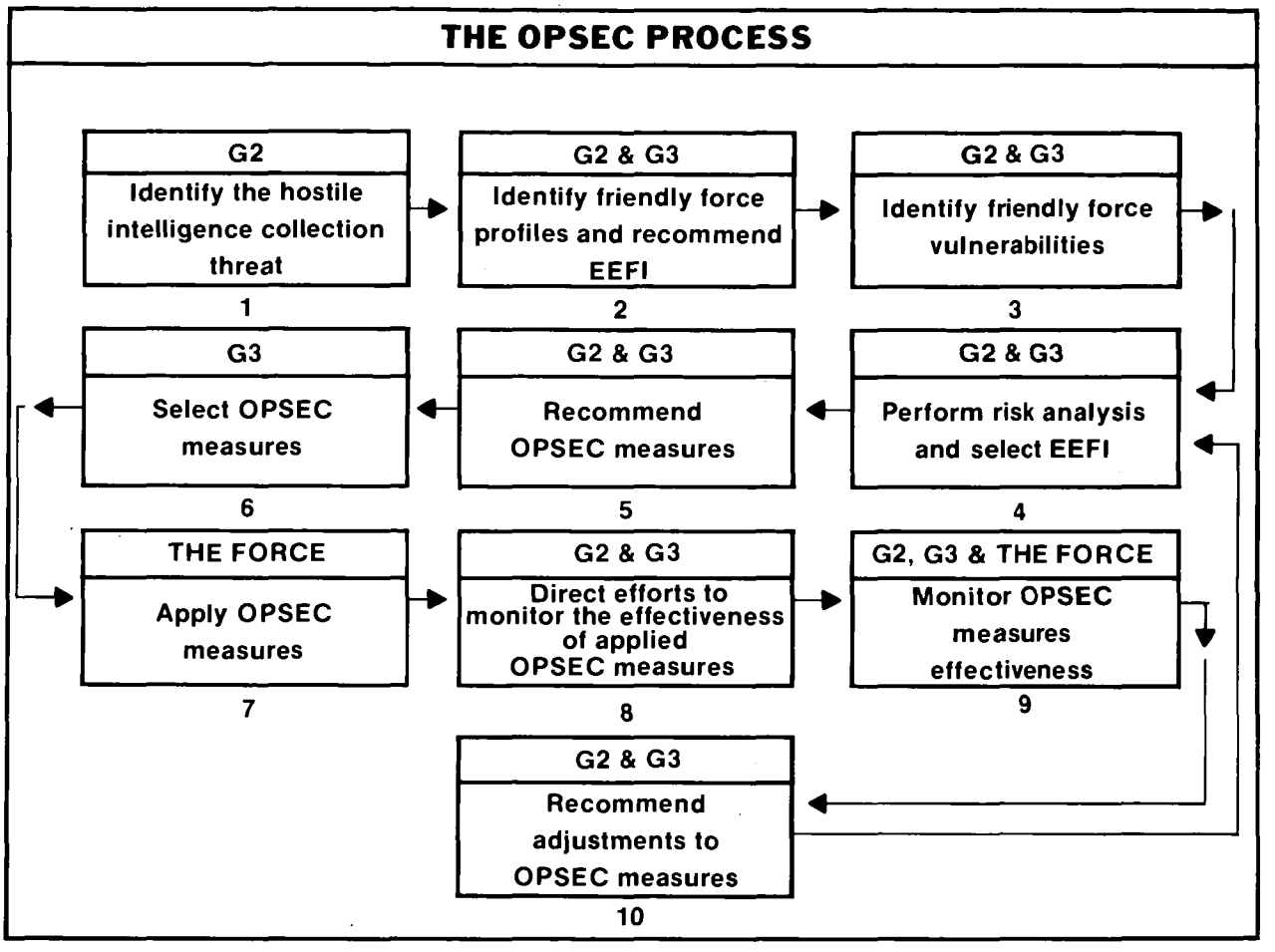
The G2, augmented by the CI analysis section, performs the detailed staff functions in support of the OPSEC program. The CI analysis section—

- ☐ Analyzes enemy intelligence capabilities.
- ☐ Assists in developing friendly force profiles.
- ☐ Maintains the intelligence threat data base.
- ☐ Assists in identifying friendly vulnerabilities to hostile intelligence collection, sabotage, and terrorism.
- ☐ Supports G3 OPSEC risk analysis.
- ☐ Recommends OPSEC measures.
- ☐ Prepares appropriate portions of CI estimates, plans, annexes, and similar documents.
- ☐ Recommends OPSEC evaluation requirements.

CI Support

CI support is a critical element in any effective OPSEC program. CI functions, performed by the intelligence staff, are integrated with the OPSEC functions of the operations staff. The following illustration describes the overall OPSEC process, identifies staff responsibilities, and demonstrates the integration of the operations and intelligence efforts.

An accurate assessment of enemy intelligence capabilities is the foundation of friendly vulnerability assessments and the development of effective OPSEC measures. Identification and assessment of the hostile intelligence threat are accomplished through a continually updated data base maintained by the CI analysis section. Information for the data base is obtained from the ASPS as a result of requested collection actions or intelligence disseminated from higher levels of command. Using all available information, the CI analysis section assesses the hostile intelligence threat



for use in later phases of the OPSEC process.

Included in the OPSEC data base are friendly force profiles made up of signatures, patterns, and indicators. These show how a unit might appear through the eyes of the enemy. The friendly force data is crucial to planning operations because it aids in developing EEFI, OPSEC measures, accurate appraisals, and effective deception plans.

Profiles are comprehensive studies of a unit and its activities to include equipment, doctrine, SOPs, and so forth. Profiles result from actions, to include the timing of those actions, taken by military units and individual soldiers. Once compiled, unit profiles provide a picture of the unit as the enemy sees it. Analysis of a unit's profiles can reveal signatures and patterns about unit procedures and, over time, may be used to determine intentions. Collectively, profiles can be used by the enemy to help predict probable courses of action. Friendly OPSEC analysts assist units to develop their profiles to determine weaknesses and recommend corrections to commanders. To do this, all unit activities must be identified to determine whether they provide indicators to the enemy. Profiles which should be maintained include—

- ☐ C2 communications.
- ☐ Intelligence.
- ☐ Tactical operations and maneuvers.
- ☐ Logistics.
- ☐ Administration and other support.

Signatures are unique characteristics of a unit which result from the presence of a unit or activity on the battlefield. Signatures are detected because various units have different equipment, are of differing sizes, emit different electronic signals, and have different acoustic, thermal (infrared), and seismic signatures. Detection of individual signatures can be grouped by analysts to show installations, units, and activities.

Patterns are stereotyped actions which habitually occur in a given set of circumstances. Military forces have SOPs for virtually everything they do. Predictable patterns may be developed by commanders, planners, and operators. Types of patterns are as numerous as there are procedures in military operations. For example, before every offensive operation the volume of communications increases dramatically and then drops off equally dramatically just before the attack. Enemy analysts would note this pattern and be able to predict a unit's intentions for all future offensives.

Indicators are bits of information concerning a military unit and its activities (much like a piece of a puzzle) which allow enemy analysis to make estimates of friendly capabilities, weaknesses, and intentions. In preparing for a tactical operation, it is virtually impossible for military forces to avoid or conceal all indicators. In many cases, these activities can be detected by the enemy and used to predict probable courses of action. Indicators that cannot be eliminated or concealed may be considered as a basis for a deception plan.

Identification and interpretation of specific indicators are critical tasks in intelligence operations whether the indicator is friendly or enemy. Intelligence people look for indicators, analyze them, and make estimates of capabilities, vulnerabilities, and intentions. These analyses lead to requests for information and planning and eventually provide the basis for decisions and orders.

Friendly force vulnerabilites are identified through comparison of friendly indicators and hostile collection capabilities. As an aid to analysis, IPB techniques are applied to friendly force patterns and signatures so we can see ourselves as viewed by enemy collection systems. For example, the range and focus of hostile collection means can be plotted on a map and, with intervisibility overlays, a determination made of what friendly activities are vulnerable to enemy observation. Further, IPB can be applied to develop OPSEC measure recommendations. For example, a map overlay could be constructed to indicate which routes minimize detection during movement, or which areas would afford concealment and cover for signature-unique equipment.

Data bases on friendly forces are continually updated as the situation changes. Changes in operations, tactics, equipment, or personnel that may alter any signatures and patterns are immediately entered into the data base.

OPSEC risk analysis is a three part process where risks to an operation are determined, OPSEC measures are identified, and then the cost of implementing those measures is compared to the benefit in terms of derived risk reduction. It is conducted and presented by the G3 to the commander for decision. The results of risk analysis include the identification of the EEFI which must be concealed from the enemy. EEFI, in turn, provide the basis for applying appropriate OPSEC measures.

OPSEC measures must be systematically developed to protect EEFI from enemy detection. Generally, there are six options for the decision maker:

- ☐ Apply one or more OPSEC measures.
- ☐ Accept risk of detection.
- ☐ Use deception.
- ☐ Change the operation enough to eliminate the vulnerability.
- ☐ Any combination of the above.
- ☐ Prohibit the activity (cancel the mission).

Based upon recommendations from the G2 concerning the capabilities and vulnerabilities of enemy intelligence systems and effective OPSEC measures, the G3 selects those commensurate with the planned operation. Selected OPSEC measures are implemented through the OPSEC annex to the OPORD.

Proper application of OPSEC measures allows essential activities to take place while at the same time reducing the probability of detection or correct enemy interpretation of their meaning. OPSEC measures are planned to protect indicators which can be collected by specific enemy collection means. Since the enemy will rely on more than one means of gathering intelligence, indicators are weighed against each collection capability.

Elements of the command implement OPSEC plans as directed in the OPSEC annex. Simultaneously, the G3, supported by the G2, identifies those OPSEC measures which should be monitored closely to determine their effectiveness. Ad hoc OPSEC evaluation teams are formed and directed to monitor the OPSEC measures concerned. Generally, the teams are comprised of personnel well-qualified in the areas under evaluation and CI personnel from the MI unit. For example, if engineer operations are to be evaluated, engineers are assigned to the team along with CI personnel. OPSEC evaluations may also be performed by unit personnel with expertise in the area being evaluated. It is not necessary to always use CI personnel as long as the subject matter expertise is used.

CI personnel assigned to the teams assist in evaluating units for identifiable patterns and signatures exploitable by the enemy. Their knowledge of enemy intelligence collection capabilities and effective OPSEC measures is critical to the effectiveness of the team. Additionally, CI personnel may assist in the interrogation of selected EPWs and refugees to determine enemy intelligence requirements and to gage the effectiveness of OPSEC measures.

During the course of OPSEC evaluations, the teams advise commanders and staffs about inadequate security practices that may compromise EEFI or provide indicators of any planned or ongoing operations. If any actions indicate possible compromise of essential information, the data is reported to the CI analysis element for analysis of the probable information disclosed and the risks to which the command may be subjected. Examples of the data to be reported include—

- ☐ Suspected disclosure of designated EEFI.
- ☐ Serious violation of established security procedures.
- ☐ Friendly losses attributable to probable compromises.
- ☐ Indications that the enemy had prior knowledge of a friendly operation.
- ☐ Enemy activity directed against otherwise well-concealed friendly vulnerabilities.

Based on the information reported, adjustments are made to the OPSEC program. When necessary, new EEFI are developed and changes to OPSEC measures prepared and disseminated.

Analysis of the OPSEC program is an ongoing activity during the operation and is continued after the operation has been completed. Post evaluation reports concerning OPSEC conditions and the effectiveness of OPSEC measures previously implemented are presented to commanders and operations officers. The detail of these reports will vary with the extent of an operation, size of unit, time available, and the current situation. The purpose of these reports is to allow analysis of OPSEC measures to determine changes necessary to improve the security of the command. Command patterns and signatures are examined for possible changes to the data base. SOP items are evaluated for effectiveness and training emphasis. OPSEC planning practices are reviewed to assure that future planning considers present weaknesses when developing OPSEC measures for operations.

OPSEC Measures Worksheets are working documents used by the OPSEC analyst to facilitate using the ten step OPSEC process. They are also used to task units for implementation of specific OPSEC measures. A sample OPSEC Measures Worksheet follows.

OPSEC MEASURES WORKSHEET							
FRIENDLY INDICATOR	HOSTILE COLLECTOR	EVAL	OPSEC MEASURES	RISKS	COSTS/ BENEFITS	RESPONSIBLE UNITS	REMARKS

SUPPORT TO REAR OPERATIONS

The primary purpose for conducting rear operations is to retain freedom of action to conduct close and deep operations. The objectives of rear operations are to—

- ☐ Secure the rear areas and facilities.
- ☐ Prevent or minimize interference with command, control, and communications (C^3).
- ☐ Prevent or minimize disruption of combat support and CSS forward.
- ☐ Provide unimpeded movement of friendly units throughout the rear area.
- ☐ Provide area damage control (ADC) before, during, and after hostile action or natural disaster.

CI supports rear operations through a variety of actions designed to defeat or assist in defeating the enemy threat to our rear areas. Each action is based on the threat posed by enemy agents, elements, and units normally used against the rear.

THREAT

Soviet military doctrine stresses attacking enemy forces throughout the depth of their dispositions. The Soviets fully appreciate the important role that unconventional warfare (UW) can play in support of the main attack. UW operations consist of a variety of military and paramilitary operations to include partisan warfare, subversion, sabotage, and terrorism conducted during periods of peace and war. It also includes other operations of a covert or clandestine nature.

Soviet UW missions can be divided into three basic categories: strategic, operational, and tactical. The principal differences in the missions are the level of C^2 used in an operation and the nature of the targets engaged. The overall objectives are similar regardless of mission category and include—

- ☐ Weakening the military capabilities of the target country.
- ☐ Supporting follow-on conventional military operations.

Strategic UW missions are controlled by the Committee for State Security (KGB). These missions, conducted in the heartland of the enemy, are aimed at reducing the enemy's ability to continue fighting and toward breaking the national will to resist.

Strategic missions include efforts to—

- ☐ Intimidate and demoralize the populace.
- ☐ Create chaos and disrupt public services.
- ☐ Undermine national resistance.

Strategic UW missions also may be performed by select regular airborne forces. These would not be normal airborne missions which generally require coordination with front-line operations, but small, elite airborne groups which operate at great depths behind enemy lines. Their basic objectives are to weaken enemy operational readiness and combat effectiveness. Their missions could include—

- ☐ Neutralization of major enemy headquarters.
- ☐ Destruction of enemy nuclear weapons.
- ☐ Sabotage to support disruption of enemy communications and key logistics.

Operational UW missions in support of the front and subordinate armies are carried out under the control of the front commander. Airborne forces, the General Staff's Main Intelligence Directorate (GRU) special purpose units, and army special purpose units would perform these missions. Their primary objective would be to destroy or neutralize enemy nuclear capabilities forward of the front to a depth of 350 to 1,000 kilometers. Additional missions include—

- ☐ Preparation and security of landing sites for regular airborne forces.
- ☐ Intelligence on the location and strength of enemy forces.
- ☐ Sabotage operations against airfields, railway lines, road and rail bridges, and communications systems.
- ☐ The use of terror to intimidate the population.
- ☐ Organization of local guerrilla or partisan groups.

Operating in the enemy rear areas, these units try to prevent effective and timely employment of reserves. They also serve to generally disrupt enemy offensive and defensive capabilities.

Tactical UW missions are conducted in support of divisions and are similar to the operational missions described above. Tactical missions are carried out on a smaller scale and directed at targets in the division's area. The Soviet divisional reconnaissance battalion has a limited capability to perform UW sabotage missions to a depth of 100 kilometers.

The Soviet leadership has a variety of elite forces for conducting UW missions: special units of the KGB, GRU, airborne, and ground and naval forces normally called special purpose forces or SPETSNAZ. Responsibility for the overall planning and coordination of sabotage actions in peace and war probably resides with the KGB. The KGB special purpose teams have a sabotage mission and are thought to be targeted primarily against the civilian sector. Their tasks would be to create general panic among the civilian population, to disrupt civil government and public utilities, and to damage or destroy key production facilities.

The regular armed forces maintain elite airborne units, special sabotage and reconnaissance units, special long-range reconnaissance units for UW missions, and SPETSNAZ forces. SPETSNAZ are intended to operate in small groups against key political, military, C^2, and transportation and industrial targets in the enemy rear area.

The potential for UW is not limited to special KGB and elite airborne units. The GRU maintains a number of small, special purpose units. These units are primarily concerned with UW activities in DS of combat operations. Their main tasks include—

- ☐ Preparing for the landing of airborne units behind enemy lines.
- ☐ Reconnaissance against nuclear delivery means, storage facilities, and other vital military targets.
- ☐ Sabotage, disruption, and neutralization of key political and military personnel.
- ☐ Possible use of NBC weapons.

A special purpose brigade is assigned to and controlled at front level. Subordinate armies and divisions have elements within their reconnaissance units that are capable of conducting long-range UW operations.

UW is primarily designed to support a surprise attack. Clandestine operations in the target area before the start of hostilities increase the probability of destruction of key targets well before rear operations measures are heightened.

US divisions and corps can expect to be confronted with a significant rear area threat regardless of where they fight. In most cases, this threat will be based on the Soviet model described in the preceding paragraphs. To counter this threat, US Army doctrine divides it into three levels and establishes procedures for dealing with each. (These levels do not correspond directly with the three levels of the Soviet UW mission.)

The ***level I*** threat includes activities of enemy agents, sabotage by enemy sympathizers, and activities of terrorist organizations. ***Level II*** includes diversion, sabotage, and reconnaissance conducted by tactical units smaller than battalion size. ***Level III*** includes airborne operations, air assault insertions, and amphibious operations of battalion size or larger.

The defeat of the threat at each level is accomplished by base defense forces and MPs deployed in the rear area. When threat activities exceed the capabilities of base defense forces and MPs (level III threat), a tactical combat force under the control of the rear operations officer (ROO) will be used to defeat the threat (see FM 90-14). CI provides support in countering all target levels; however, CI is most effective in providing indications and warning regarding level I and level II threat activities.

RESPONSE

CI support to rear operations includes those functions performed in support of OPSEC. It also includes a number of other functions normally not accomplished in support of the OPSEC mission.

CI personnel conduct liaison with local police and intelligence agencies, both military and civilian, to foster a spirit of cooperation and to obtain information. Generally, liaison is established in peace and carried over into war. The cooperation obtained from such agencies through liaison efforts is critical to neutralizing the level I threat.

The CI analysis section creates and maintains black, gray, and white lists to permit rapid identification of key indigenous personnel in rear areas. Persons on black lists are those personnel whose capture and detention are of prime importance to the US Army. They include known or suspected agents, saboteurs, enemy sympathizers, and others who represent a serious threat to rear area security. Gray lists contain the identities and locations of those personalities whose inclinations and attitudes toward the political and military

objectives of the US are obscure. Regardless of their political inclinations or attitudes, personalities may be listed when they are known to possess information or particular skills required by US forces. They also may be individuals whose political motivations require further exploration before they can be of use to US Forces. White lists contain the identities and locations of individuals who have been identified as being of intelligence or CI interest. They are expected to be able to provide information or assist in collecting needed data. Persons listed on white lists usually are in accord with, or favorably inclined toward, US policies. Contributions are based on a voluntary and cooperative attitude.

CI teams identify and assist in neutralizing UW teams and cells, an important priority in rear operations. Information provided by CI personnel is passed to local police or military forces, US MPs, or other US combat elements.

CI personnel also conduct defensive source operations (DSOs) to provide I&W information on potential hostile rear area activity and to provide leads for the identification of perpetrators of incidents against friendly units and personnel. The sources are personnel who serve as paid or unpaid informants. They are generally local national employees such as barbers, facilities engineers, and others whose access to the military and civilian communities may permit them to become aware of potential activities against friendly facilities.

CI teams conduct incident investigations of suspected sabotage, subversion, and espionage directed against the rear area. These investigations can lead to the identification and elimination of perpetrators of hostile actions in the rear area. Pattern analysis of multiple incidents can reveal enemy plans and intentions.

CI teams conduct tactical HUMINT operations to exploit captured personnel who can identify other hostile agents and saboteurs, pinpoint team locations, or provide other information. Time constraints generally preclude extensive tactical HUMINT operations, but enemy agents, sympathizers, and terrorists can often be neutralized.

CI personnel also are used to support terrorism counteraction. The role of CI in countering terrorism is primarily to identify the threat including terrorist organizations, capabilities, tactics, and targets. Army CI activities, in respect to counterterrorism investigations, involve a close working relationship with criminal investigation elements, the provost marshal's office, indigenous police, and allied intelligence agencies. Crisis management teams (CMT) consisting of various military staff sections include CI personnel to advise and assist the commander in the event of terrorist incidents. Information relating to terrorist activities is gathered by the CMT intelligence representative from local sources and through liaison with INSCOM elements.

Each CI function conducted to support the security of the rear area is controlled and coordinated by the G2 for maximum effectiveness. The results of these actions contribute to the success of close and deep operations. Security of the rear area permits the uninterrupted flow of support to the combat forces deployed forward, an action critical to sustaining the fight. Additionally, the counterespionage functions of CI contribute directly to the OPSEC of the entire force and, in some cases, levels of command above that at which the functions are carried out.

SUPPORT TO DECEPTION

BAT-D includes all actions at ECB taken to mislead the enemy into actions which are counter to enemy interests. Based on the G3's recommendation, the commander selects a deception objective. The operation includes manipulating, distorting, or falsifying information available to the enemy to

ensure security of actual plans, operations, or activities. Generally, deception operations closely parallel actual operations and require a high degree of security through the application of effective OPSEC and other support to achieve effectiveness. Part of the support provided is CI. CI supports deception with—

- Analysis of the intelligence threat.
- Recommendations of deception measures.
- Support to the security of the deception and the actual operation.
- Evaluation of the implementation of deception measures.
- Evaluation of the effectiveness of the deception.

Analysis of the enemy intelligence system is the critical element of any deception. Analysis is performed on the information maintained in the hostile intelligence collection data base, which is used for both OPSEC and deception. When this analysis is accomplished for OPSEC purposes, it focuses on enemy capabilities. When supporting deception, it focuses on enemy intelligence vulnerabilities. CI analysis of the enemy intelligence system determines—

- The types of collectors, their capabilities and limitations, to which false information must be presented.
- The minimum requirements for realism in deception measures.
- The strengths and weaknesses of enemy intelligence analysis to further determine the amount of information needed for the enemy to draw appropriate conclusions.

The deception operation must achieve a delicate balance in the amount of true and false data the enemy is permitted to collect. Enough data must reach the enemy analyst to allow conclusions to be drawn about our apparent intentions without raising suspicions about the deception itself. The CI analysis attempts to identify exactly which elements of information should be exposed to enemy collection and the most effective, least suspicious way of presenting each element.

Based on the analysis of the enemy's intelligence system and its comparison with the deception objective, the CI analysis section prepares recommendations for deception measures. Generally, detailed coordination (based on a need to know) is conducted with other elements of the intelligence staff before the recommendations are presented to the G3.

Security is critical to the effectiveness of the deception. CI supports the OPSEC measures taken in conjunction with the deception to protect factual information from enemy intelligence collection. It also supports the OPSEC measures taken to protect the deception itself. The enemy must be convinced that the intelligence collected and processed is valid. Therefore, all indications of a deception must be suppressed.

CI teams are used as part of ad hoc teams to monitor the implementation of deception measures. Their expertise in enemy intelligence capabilities and limitations is critical to determining the probable effectiveness of deception measures. The presence of unit experts on these teams is even more critical for deception operations than for OPSEC evaluations. Only those personnel familiar with a unit's operations will know if the deception measure appears realistic.

The CI analysis section, in coordination with the G2 and the ASPS, evaluates the effectiveness of the deception throughout the operation. When necessary, and only after thorough analysis of the situation, the section makes recommendations for adjustment of the deception plan. The final decision and responsibility for implementing such changes rests with the G3.

SUPPORT TO COMMAND, CONTROL, AND COMMUNICATIONS COUNTERMEASURES

C^3CM tasks are designed to prevent the enemy from being able to decisively concentrate his combat power. They are designed to isolate the enemy commander from his means of battle synchronization at the same time that he experiences a C^3 crisis. Timed to fit the friendly commander's operational plan, C^3CM can help create the moment to seize the initiative. C^3CM tasks also involve those actions which cause enemy decision times to be lengthened, as well as to cause faulty decisions. C^3CM measures may be direct or indirect. Direct measures include attacks against the means (functions) used to control elements of combat power. They include not only troop control centers, weapons system control centers, and weapons direction means, but RSTA control centers and REC systems as well. Indirect measures which lead to the inability of the enemy commander to effectively concentrate combat power are deception and OPSEC.

For much too long, the enemy's intelligence systems have been ignored when identifying targets for destruction within the C^3CM strategy. With the sophistication of the sensors on the modern battlefield, this is no longer a possible option. Survivability of our military forces depends heavily on the elimination of the enemy's "eyes and ears" or on keeping collected information from reaching the enemy commander. Anti-intelligence warfare is designed to do just that.

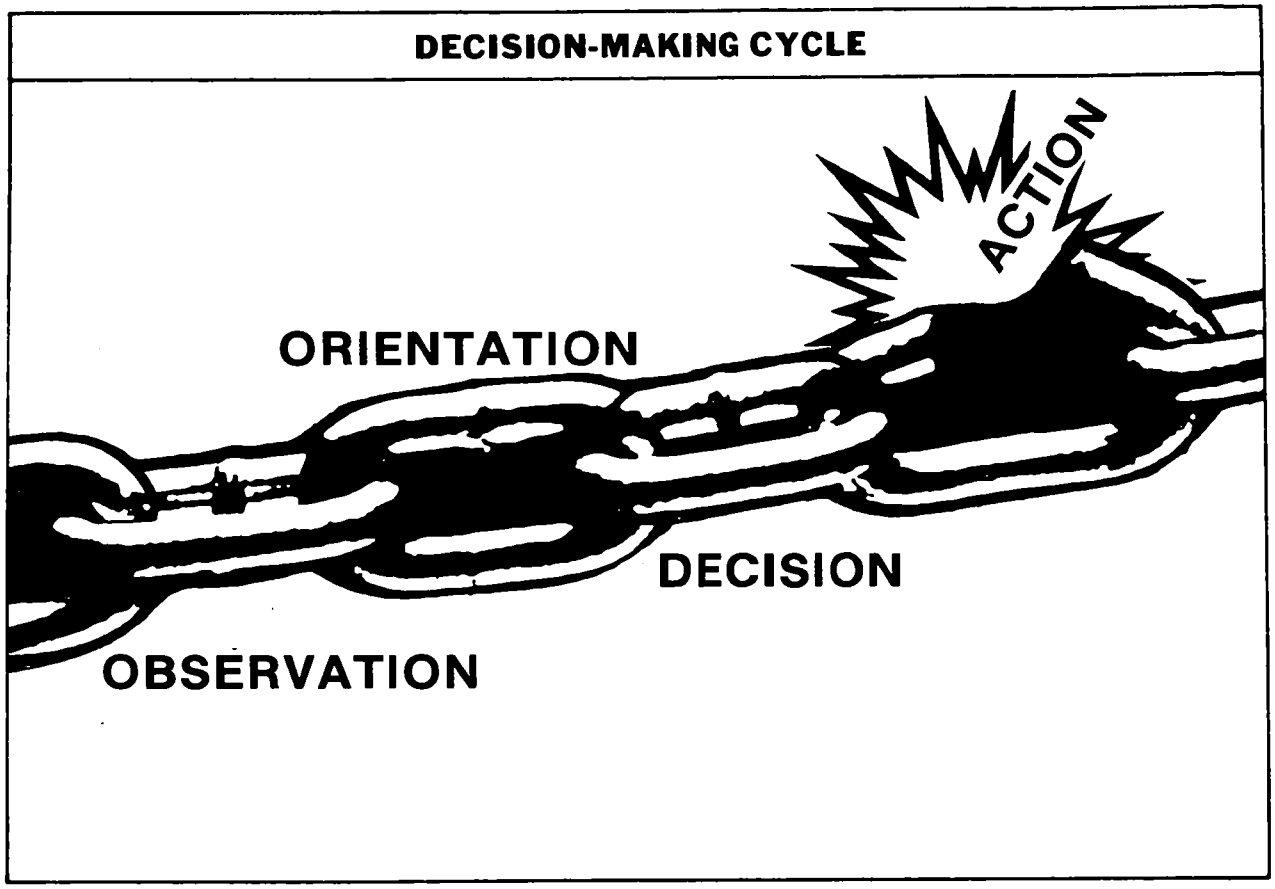
Counterintelligence support to C^3CM integrates age-old principles of combat to effectively prevent the enemy's intelligence systems and decision-making cycle from completing the circuit needed to take action against friendly forces. (See the following illustration.)

The first two links of his decision-making chain (observation and orientation, or his collection and analysis capabilities) are the targets of the offense-oriented, extremely aggressive CI support to C^3CM program.

The first step to accomplish the goals of CI support to C^3CM is to completely identify the threat. What sensors does the enemy have; where are they located; how and when does the enemy use them; and what are their specific capabilities? These are all questions which must be answered. The same types of information must also be identified for his intelligence data processing and analysis elements.

Once the threat is completely understood, the commander must allocate resources, such as infantry, artillery, armor, or EW systems to destroy or significantly degrade the key sensors or processing nodes at the most critical points of the battle.

At the same time, the theme must be proliferated to our combat elements that enemy REC and RSTA systems must be engaged when encountered on the battlefield. Enemy REC and RSTA systems have unique physical signatures and are normally fielded in thin-skinned vehicles. Such soft targets are thus easily neutralized. They should be engaged on sight, since the payoff for their destruction is considerable.


DECISION-MAKING CYCLE
ACTION
ORIENTATION
DECISION
OBSERVATION

CHAPTER 5

Electronic Warfare

Modern combat forces depend heavily on electronic devices to acquire and distribute information and to command and control forces and weapons systems. Each new electronic device increases the ability of the commander to apply combat power. It also brings with it a susceptibility to exploitation and disruption. EW is a vital element of C^3CM. Specifically, EW is the means through which commanders protect their own electronic systems while attacking those of the enemy. It integrates the offensive use of jamming, electronic deception, and support to physical destruction to degrade, influence, or destroy enemy electronic capabilities. EW is conducted within three broad mission areas of C^3CM—defend, degrade or disrupt, and deceive.

The defend mission is accomplished through the use of ECCM to protect our use of electronic systems. ECCM are the responsibility of every soldier who uses or supervises the use of radios, radars, or other electronic equipment. ECCM are described in FM 24-33. Defending is also supported by ESM and ECM. ESM locate enemy jammers for destruction while friendly jammers can be used to screen friendly communications from the enemy.

Enemy use of electronic systems is disrupted through destruction, jamming, or deception. The goal is to completely disrupt enemy activities. However, the small number and vulnerability of jammers available generally limits their use to critical targets that have significant impact on the enemy. Disruption is fully supported by intelligence and ESM activities that identify, locate, and provide technical information on HVT.

The deception mission is accomplished by feeding false or misleading information to enemy electronic sensors or by transmitting it directly into operational channels. Electronic deception generally is part of an overall deception plan. This ensures that what the enemy collects electronically agrees with, or at least does not refute, the indicators presented by other deception measures.

This chapter describes the planning and targeting of ESM and ECM—the offensive components of EW. It emphasizes ECM techniques to provide an understanding of ECM employment. ESM, although a critical element of EW, are not described in detail as these operations are conducted the same as other collection operations described in Chapter 3.

ELECTRONIC WARFARE SECTION

The EWS is a critical element in accomplishing the EW mission of the command. It augments the G3 staff with the necessary personnel and expertise to perform the detailed planning, target selection, and coordination that are required for EW success.

The EWS deploys and operates as an integral part of the G3 staff. The primary function of the EWS is mission management of ECM, to include both jamming and electronic deception. The section determines ECM requirements based on guidance from the G3 and plans and coordinates the actions necessary to satisfy each requirement. The EWS assists in preparing EW estimates and annexes and developing ECM mission tasking.

The EWS assesses enemy vulnerabilities, friendly capabilities, the friendly mission, and the friendly EW strategy. The section then targets those enemy nets and emitters that pose the greatest threat to the friendly mission. These targets are assigned a priority and nominated for attack by fire, maneuver, jamming, or deception. ECM techniques are described in the following section to provide a basis for understanding how targets are attacked electronically.

To fully integrate ECM with the commander's scheme of fire and maneuver, the EWS must maintain a close, continuous working relationship with other staff sections and elements within the division TOC and the MI battalion TOC. The key to the coordination process is the presence of officers trained in EW operations in most of these elements. This provides a common basis for understanding the potential uses, capabilities, and limitations of EW. Equally important is that EWS personnel be knowledgeable of the mission of the command and the functions and responsibilities of the elements with which they coordinate. The following chart depicts EWS coordination requirements.

ELECTRONIC COUNTERMEASURES

ECM are of two types—jamming and deception. Through jamming, the passage, receipt, or gathering of information by electronic means is prevented or disrupted. Electronic deception feeds false information to the enemy, either through their electronic collection devices or directly to their electronic systems. All types of electronic equipment are vulnerable to both jamming and deception. The following descriptions focus on radio communications and radar systems because they are the most numerous. Other systems such as missile guidance, telemetry, and navigational aids may

EWS COORDINATION REQUIREMENTS

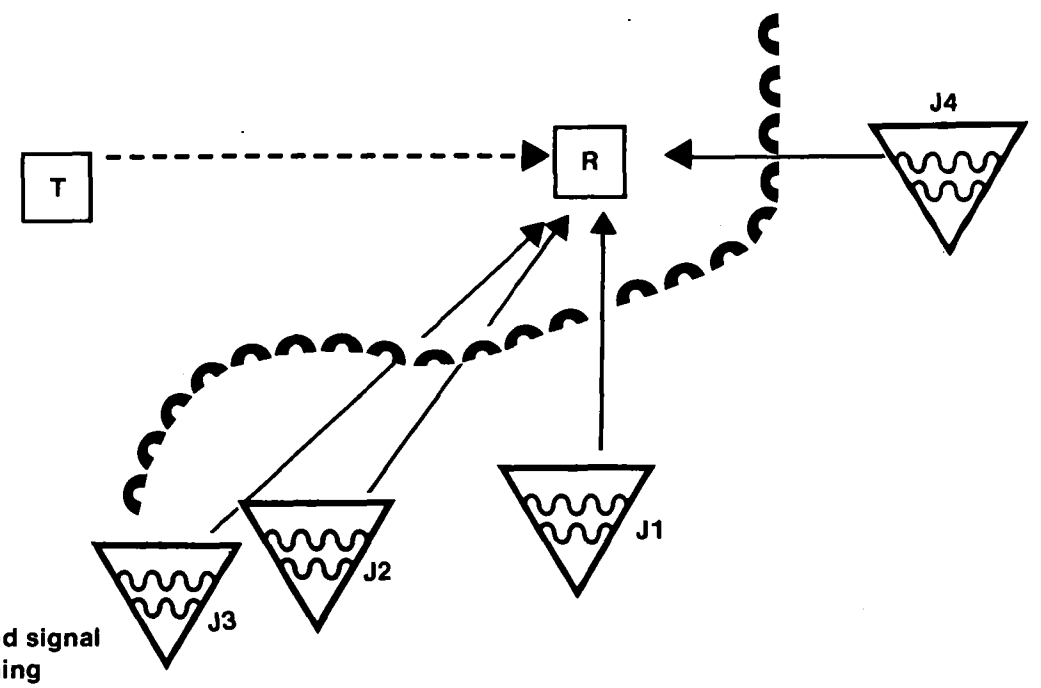
SECTION/ELEMENT	COORDINATION
G3 Staff	Friendly situation Planned operations Target priorities
Fire Support Element	HVT identification Integrate jamming and fires
C-E Officer	MIJI feeder report evaluation TABOO, PROTECTED frequencies Electronic deception ECCM planning ECM effects on friendly C-E ECM support to ECCM
CM&D Section	Mission tasking ESM requirements to support ECM GUARDED frequencies Jam or listen decisions
OPSEC Staff Element	Electronic deception ECCM
ASPS	Electronic OB Enemy situation Enemy capabilities } Electronic preparation of the battlefield
TCAE	Asset status Technical data Effectiveness assessments

be of equal, greater, or lesser importance depending on the tactical situation, and the need to counter a specific enemy capability. The ECM techniques listed herein are fully described in FM 32-16.

JAMMING

Jamming is the deliberate radiation or reradiation of electromagnetic energy to prevent or degrade the reception of information by a receiver. Radio and radar receivers tuned to a given frequency are jammed by delivering more power to the receiver to prevent the receiver from receiving its intended signal. In general, the effectiveness of jamming depends on relative power between transmitter and jammer; relative distance between transmitter, jammer, and receiver; on terrain barriers; and on whether or not the receiver is using a directional antenna as shown below.

JAMMING



-- intended signal
jamming
T - transmitter
R - receiver
J - jammer
J1 - needs less power than T to jam R
J2 - needs the same power as T
J3 - needs much more power than T
J4 - needs the same power as T (can be defeated by R using a directional antenna)

Communications jamming interferes with enemy communication systems. It may be applied to secure communication systems to force the enemy to transmit in the clear so that the communications can be exploited for combat information. Jamming also can aid in DF by forcing the enemy to transmit longer, allowing time for tip-off and multiple LOB from different locations for position determination. When not dedicated to jamming missions, jammers are used in an ESM role to intercept communications. Care should be exercised when using jamming systems for ESM. Damage to power units and equipment may occur if an ECM system is used for a prolonged period for ESM.

Noncommunications jamming is directed against such electronic devices as radar, navigation aids, and guidance systems. The Army does not currently possess a noncommunications jamming capability. Such support must be obtained from Air Force assets.

Jamming against communications equipment is accomplished using spot, sweep, or barrage jamming.

Spot jamming may be directed at a single frequency or multiple frequencies through—

- ☐ Sequential spot jamming, in which various frequencies are jammed one at a time, in sequence.
- ☐ Simultaneous multi-spot jamming, in which several frequencies are jammed at the same time.

In both spot and sequential spot jamming the full power of the jammer is directed against one frequency at a time, which increases the effectiveness and range of the jammer. Multi-spot jamming is directed against more than one frequency. Spot jamming is less apt to interfere with friendly frequencies that are close to the frequency being jammed. The main disadvantage is that receivers can easily avoid spot jamming by slightly changing (detuning) the frequency they are receiving. Soviet radios have continuous tune capability while most US equipment uses detent-tuned frequency settings.

In sweep jamming, the jammer goes through a frequency range then repeats the sweep continuously. All frequencies in the range are jammed and friendly frequencies may be affected.

Barrage jamming spreads the jammer's power over a much larger portion of the frequency spectrum than spot jamming, thereby reducing the radiated power directed at any single target frequency. It is similar to sweep jamming because there are no frequencies free of jamming within the targeted portion of the spectrum.

The advantage of barrage jamming is that more frequencies can be jammed at the same time. The disadvantages are that friendly frequencies may be jammed. Also, spreading the jammer's power over a greater portion of the spectrum reduces the amount of power available to jam each frequency, reducing the effectiveness and range of the jammer.

The jamming signal may be varied by amplitude, frequency, or pulse with an almost unlimited variety of modulating signals. The type of signal used is determined by the capability of the jamming equipment, the nature of the signal to be jammed, and the desired result.

Reradiation jamming is accomplished by using special equipment to receive enemy transmissions, alter them in some way, and reradiate (retransmit) the signal back to the enemy. There are two types of equipment used for this purpose. They are—

- ☐ Repeaters, which intercept the enemy signal, alter it, amplify the altered version, and retransmit it.
- ☐ Transponders, which automatically transmit a predetermined signal in response to the reception of a given signal.

The principal targets of reradiation jamming are radars and navigation aids. The Army currently has no reradiation jammers, since these systems are primarily used by aircraft which must penetrate the FLOT.

Another reradiation jamming method is reflection jamming. Also called mechanical

jamming, it is used to confuse enemy electronic systems. It causes those systems to receive false targets, thereby degrading system effectiveness. The most common types of reflective jammers are—

- Chaff, which consists of narrow metallic strips of various lengths and frequency responses. It is primarily used to defeat antiaircraft radar by reflecting radar echoes to the receiving components of the enemy system.
- Rope, a form of chaff, which consists of a long roll of metallic foil or wire designed for broad, low frequency response.
- Corner reflectors, which consist of flat reflecting surfaces connected to form a three-dimensional reflector. Corner reflectors reflect a strong return to radar, thus enhancing the radar signature of the object. When using corner reflectors, small boats at sea appear larger on radar screens, and small vehicles can appear to be tanks.

DECEPTION

Electronic deception is employed to cause the enemy to misinterpret what is received by electronic systems. Normally, it is conducted as part of a larger deception operation and is seldom, if ever, conducted alone. It involves actions associated with friendly electromagnetic radiations (manipulative electronic deception (MED), simulative electronic deception (SED)), and, with those of the enemy force (imitative electronic deception (IED)).

MED and SED are accomplished by non-MI elements of the force. The C-E officer plays a major role in planning and executing MED and SED. Because of its technical requirements, IED is accomplished almost exclusively by MI elements.

MED is conducted by altering the electromagnetic profile of friendly forces. It seeks to counter hostile EW and SIGINT activities by manipulating friendly electromagnetic emissions. This is done by modifying the technical characteristics and profiles which would provide an accurate picture of friendly intentions, or by deliberately transmitting false information.

The objective of MED is to have the enemy ESM and SIGINT analysts accept the profile or information as valid and thereby arrive at an erroneous conclusion concerning friendly activities and intentions. There are two basic forms of MED, manipulative communications deception (MCD) and manipulative noncommunications deception (MNCD).

MCD requires a complete knowledge of the friendly force communication signature over an extended period of time and in a variety of combat situations. Enemy analysts look for deviations from the US and allied communications norms before and during all situations. When isolated, these deviations may become indicators of projected actions by US and allied forces. MCD techniques include—

- False traffic levels.
- False peaks.
- Padding.
- Routing.
- Electronic cover.
- Controlled breaches of communication security (COMSEC).

MNCD applies the same principles as those in communications deception. The technique differs only in the type of equipment used. The activity of noncommunications emitters is increased or decreased to imply a like change in the activity of the unit. Both MCD and MNCD depend heavily on the friendly C-E and SIGINT/REC data base developed by unit counter-SIGINT or CI analysis personnel.

SED is conducted to mislead the enemy as to the actual composition, deployment, and capabilities of the friendly force. It seeks to counter hostile EW and SIGINT efforts by simulating nonexisting units or capabilities, or by simulating actual units or capabilities at false locations. Both communications and noncommunications

equipment may be used in the simulation, depending on the type of deception being projected to the enemy. SED tactics include—

- Unit simulation. A network of communications and noncommunications emitters is established and operated to match those emitters and activities found in the type unit or activity being simulated.
- New or different equipment capability simulation. The electronic signature of new or differing equipment is projected by an actual or simulated unit to mislead the enemy into believing that a new capability is being introduced into the friendly force.
- False location simulation. The electronic signature of a unit is projected from a false location while the signature from the actual location is suppressed.

IED is conducted against both communication and noncommunication emitters. Imitative communications deception (ICD) injects false and misleading information directly into enemy communication networks. The communications imitator gains admission as a bona fide member of the enemy communications system and maintains that role until the desired false information is passed to the enemy. Extreme care is exercised in entering the enemy communications system because each emitter produces its own particular signature. The friendly ICD emitter must approximate closely the enemy signature. If friendly ICD operations are unmasked, the enemy is provided an indication of US and allied forces COMINT success. With this information, enemy forces may increase their COMSEC efforts to impede the intercept and analysis of their communications resulting in loss of COMINT by US and allied forces.

ICD varies in scope based on the sensitivity of the intelligence and the sophistication of techniques and equipment used. It includes—

- Nuisance intrusion.
- Planned message intrusion.
- Cryptographic intrusion.
- Deceptive jamming.

All but nuisance intrusion require extensive technical support and specially skilled operators. Nuisance intrusion requires only compatible radio equipment and foreign language ability. All require specific authorization.

Imitative noncommunications deception (INCD) is conducted for the same purpose as ICD. It involves the introduction of radiations into the enemy's electronic system to imitate their emissions and to confuse or deceive them. The variety of target acquisition, surveillance, and electronic reconnaissance systems deployed in the battle area produces individual signatures for each class of equipment that requires unique INCD capabilities.

Some enemy radars can be deceived by repeaters, reflectors, and transponders which substitute an altered or generated signal in imitation of the radar's normal return echo. Successful deception requires a much better knowledge of the characteristics of the enemy radar than that required for jamming operations. However, if successful, IED is more effective than jamming. When repeaters and transponders are used in a jamming role, enemy forces soon discover that their operational difficulties are caused by jamming and employ ECCM to defeat it. When the same equipment is used in an INCD role, it is difficult for enemy forces to perceive the deception because their equipment appears to be functioning in a normal fashion. At the same time, the subtlety of deception effects versus those of jamming makes it more difficult for us to evaluate the effects of deception operations.

INCD techniques include—

- False target generation or spoofing.
- Range gate pull-off.
- Scan rate modulation.
- Inverse gain modulation.

ELECTRONIC WARFARE TARGETS

The targets for offensive EW are selected based on the operational requirements of each command and the enemy emitters arrayed against it. Through the target development process described in Chapter 3, critical nets and emitters are identified and targeted for destruction and electronic attack.

ATTACK OPTIONS

EW plays a major role in C^3CM actions of the command. The EW mission areas described earlier directly relate to three of the four C^3CM mission areas. The fourth, destruction, is supported by targeting data collected through ESM. C^3CM coordinates the use of destruction, jamming, and deception into a single, unified attack on enemy C^3 by the Army, Air Force, and other services.

Specific C^3CM objectives are to—

- ☐ Degrade and disrupt enemy C^2.
- ☐ Destroy, degrade, deceive, and discredit the enemy intelligence system.
- ☐ Protect friendly C^3 by degrading the enemy's ability to exploit, disrupt, or destroy it.

Supporting C^3CM and EW are intelligence and the G2. The G3 directs both efforts but does so in close coordination with the G2. This focuses efforts on HPT to magnify the value of violence, shock, and uncertainty on the enemy.

The preferred option for attacking enemy C^3 is destruction. However, there are four electronic options—intercept, locate, jam, and deceive. Although normally separate functions, some options may be executed concurrently. An enemy communications link can be jammed while the transmitting station is being intercepted and located for destruction. Electronic deception may be applied to compound the disruptive effects of jamming.

Intercepting provides combat information and technical data on the enemy's electronic systems as well as raw data for processing into intelligence. Signals are intercepted to determine their function and for technical data to support jamming and electronic deception. Signal parameters are measured and analyzed to determine the type of emitter and its battlefield function.

Locating, or DF, provides approximate locations of enemy radio and radar antennas. This facilitates the use of directional antennas in jamming operations and, when combined with other information such as terrain analysis, may provide targeting-quality data.

Jamming disrupts the receipt or exchange of orders and battlefield information. It can delay the enemy long enough for the friendly commander to exploit a situation that otherwise would have been corrected. For maximum effect and survivability, jamming is used sparingly. The jammer is activated only when necessary to disrupt vital enemy communications. Jamming provides a nonlethal alternative or supplement to attack by fire and maneuver and is particularly well suited for targets that cannot be located with targeting accuracy or that only require temporary disruption.

Electronic deception provides false information to the enemy through electronic devices to induce them to act counter to their best interest.

The following tables identify types of enemy communications nets and noncommunications emitters for interception, location, or jamming. Deception is an alternative method of attack in all instances. The distances are representative guides. Actual distances will vary based on equipment, terrain, and the tactical situation.

Generally, communications and noncommunications systems of combat elements near the FLOT are located for destruction or jamming. These options are most effective near the FLOT. Communications between planning elements, generally found well beyond the FLOT, are usually located and intercepted for intelligence. The value of information from enemy communications at the planning levels may outweigh the impact of destruction or jamming making intercept the preferred option.

ELECTRONIC OPTIONS

COMM NET BY ECHELON	FIRST ECHELON						SECOND ECHELON		FRONT
Distance from FLOT (km)	0-3	3-6	6-9	9-15	15-20	20-30	30-50	50-100	100-Up
Command and Control	INTCP LOCATE	JAM INTCP LOCATE	JAM INTCP LOCATE	JAM INTCP LOCATE	INTCP LOCATE	INTCP LOCATE	INTCP	INTCP	INTCP
Rocket and Artillery and Associated TA	JAM LOCATE	JAM LOCATE	JAM LOCATE	LOCATE JAM	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE
SSM				LOCATE	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE
Air Defense	JAM LOCATE	JAM LOCATE	JAM LOCATE	JAM LOCATE	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE
Intelligence	JAM LOCATE	JAM	JAM	JAM LOCATE	INTCP	INTCP	INTCP	INTCP	INTCP
Jammers	LOCATE	LOCATE	LOCATE	LOCATE					
Engineers	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE	INTCP	INTCP	INTCP	INTCP
CSS	JAM LOCATE	JAM	JAM	JAM	INTCP	INTCP	INTCP	INTCP	INTCP

NONCOM RADAR BY ECHELON	FIRST ECHELON						SECOND ECHELON	FRONT
Distance from FLOT (km)	0-3	3-6	6-9	9-15	15-20	20-30	30-100	100-Up
Air (SAM & AAA) Defense	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE	PRIMARY AF RESP	PRIMARY AF RESP
Weapons Locating	LOCATE	LOCATE	LOCATE	LOCATE				
Noncom Jammers	LOCATE	LOCATE	LOCATE	LOCATE	LOCATE			

NOTE: These options change little during contact in either the attack or the defense

ENGAGEMENT RULES

Commanders are authorized to employ EW forces, equipment, and techniques to support assigned missions in accordance with the following rules of engagement. The employment of—

- ESM are authorized at all times.
- ECM are authorized when the conditions specified in AR 525-22(S) are met.
- ECCM are authorized at all times in accordance with applicable security guidance for specific weapon systems.

ELECTRONIC WARFARE PRINCIPLES

EW operations are planned and conducted according to certain basic principles. These principles are supportive of the IEW principles described in Chapter 1.

INTELLIGENCE SUPPORT

Successful ECM planning and execution is fundamentally dependent on the quality and timeliness of supporting intelligence and ESM data. All-source intelligence aids in determining enemy vulnerabilities, selecting targets and priorities, and evaluating the effectiveness of actions taken. Intelligence operations—

- Correlate the various signatures, identifying the target.
- Determine target operational status, criticality, and vulnerability.
- Locate the target accurately, when required.
- Disseminate target identity and location.
- Provide technical data required for jamming and deception.

FIRE AND MANEUVER INTEGRATION

EW is only one facet of C^3CM and combined arms warfare. To achieve their full potential, ESM and ECM operations must be planned and executed as an integral part of the combat power of the force. Maximum shock effect is achieved through a well-coordinated attack on the enemy by fire, maneuver, jamming, and deception.

RESOURCE USE

EW resources always are given a standard mission such as DS, GS, general support reinforcing, or reinforcing. Their relatively low density, in comparison to the potential number of targets on the battlefield, dictates that they be used to the maximum extent possible. They are never held in reserve.

JAMMING CONTINUITY

Continuity of operations is essential if jamming is to have the desired effect on the enemy. Combat losses, equipment failure, degraded or lost C^2 and displacement may cause frequent reordering of priorities. Continuity of operations is provided through—

- Preplanned and targets of opportunity target lists.
- Backup (redundant) coverage of high priority targets.
- Planned leapfrog movement of jammers.
- Primary and alternate means of communication with jammers.
- Positive and negative control frequency lists.
- Training for worst-case situations.
- Alternate jamming using two or more jammers.
- Imaginative use of airborne jammers during fast-moving situations.

FLEXIBILITY

EW resources must have the flexibility to respond to tasking from higher echelons when operating forward in brigade and battalion task force areas. The required degree of flexibility is established through the assignment of a support relationship as described in Chapter 6.

MOBILITY

System survivability and the ability to provide sustained support in a fast moving operation are directly affected by mobility. Therefore, EW systems placed in support of a command must be as mobile as the supported command.

ELECTRONIC WARFARE PLANNING

Planning is crucial to the success of EW operations. The effectiveness of EW is dependent on the degree to which it is integrated with the commander's scheme of fire and maneuver. Full integration is best achieved by systematic planning and full understanding of employment factors.

The G3 supervises the integration of ECM into the scheme of fire and maneuver. The EWS, FSE, and G3 staff operate together to plan the attack of HVT and support the commander's concept of operations. When ECM will improve the effectiveness of fire support it is employed together with fire. Since fire support requires more accurate target location, jamming may be the preferred attack means for certain targets. Other ECM operations are planned to disrupt enemy C^2 at certain critical times. Formats and descriptions of EW target lists and worksheets used in planning are provided in Appendix F.

IPB is used throughout the EW planning process. Templates are used to focus EW operations on identified HPT and to determine defensive EW measures to defeat enemy counter-C^3 efforts. IPB applications and HPT determination are described in Chapter 3.

During the planning process, electronic HPTs are divided into four general categories for attack. These include—

- ☐ HPTs that will be located for destruction.
- ☐ HPTs that will be jammed.
- ☐ Enemy emitters that will be intercepted for combat information or intelligence.
- ☐ Enemy elements that will be deceived.

The categorization of specific enemy elements is made by the G3 assisted by the EWS and other staff elements in their particular areas of expertise. This facilitates further planning and ensures that all HPTs are attacked with the optimum means available. The nature or importance of the target may dictate that several means be employed in a combined attack.

CONSIDERATIONS

EW planning follows the normal staff planning process. It begins with the mission and commander's guidance which lead to the development of an EW estimate and annex. Planning is based on the principles of EW and the following considerations:

- ☐ Priorities.
- ☐ Technical effectiveness.
- ☐ Jammer deployment.
- ☐ Communications.
- ☐ Jammer controls.

Priorities

The many HPTs anticipated on the battlefield will generate competing demands for EW support. These demands will always exceed the MI unit's capability to respond. The commander must establish priorities among the types of targets selected for attack. These priorities are guidelines by which the G3 or S3 manages the EW planning and coordination process.

Although the tactical situation may require frequent reordering of priorities, the following are used as guidance for establishing initial priorities:

- ☐ First Priority—Protect friendly C^3 systems.
- ☐ Second Priority—Attack enemy artillery, rocket, and surface-to-surface missile (SSM) forces.
- ☐ Third Priority—Degrade or locate for destruction enemy air defense elements.
- ☐ Fourth Priority—Disrupt critical enemy C^3 links.

The outcome of the battle depends largely on the commander's ability to control friendly forces and weapon systems electronically. This is accomplished, in part, by locating enemy jammers and target acquisition systems for destruction, screening friendly communications transmitters from enemy SIGINT efforts, and strict adherence to CEOI and COMSEC procedures. It is

essential that the commander retain the capability to control. It is equally essential that combat information flow without jamming interference.

EW degrades enemy rocket and artillery capabilities by locating communications and target-acquisition means for destruction and jamming. SSM, artillery, multiple rocket launcher, and antitank units operate well forward within range of our jammers.

Joint suppression of enemy air defenses (JSEAD) is the responsibility of both ground and air forces. JSEAD is critical to cross-FLOT heliborne operations, as well as to support friendly CAS. EW support of JSEAD is a two-phased operation. First, enemy air defense systems that pose an immediate threat to friendly air operations are located and either destroyed or jammed. Second, critical elements of the enemy air defense system are identified, located, and destroyed.

The enemy uses command nets to transmit combat orders between a superior and immediate subordinates, or, in a skip-echelon mode, two echelons down. Regimental command nets are good ECM targets since they represent the link between the planners at division and the fighters at battalion. Jamming is particularly effective in close operations when the enemy is forced to deviate from a set plan. It degrades enemy ability to move, reorganize, and deliver fire on target. Timing is a key factor as the value of jamming is very short-lived.

Effectiveness

Jamming effectiveness is governed by the following technical factors. The most important of these are the distances of the target receiver from the jammer and between the transmitter and receiver of the targeted enemy communications. The technical factors are—

- ☐ Target link distance. This is the distance between the enemy transmitter and receiver. For example, it is the distance between a regimental CP and a subordinate battalion CP.
- ☐ The distance between the jammer and the enemy receiver.
- ☐ Radio LOS between the jammer and the targeted receiver.
- ☐ Antenna polarization.
- ☐ Effective radiated power of the jammer and the enemy transmitter.
- ☐ Compatible bandwidths between the jammer and enemy transceiver.
- ☐ Weather, terrain, and vegetation.

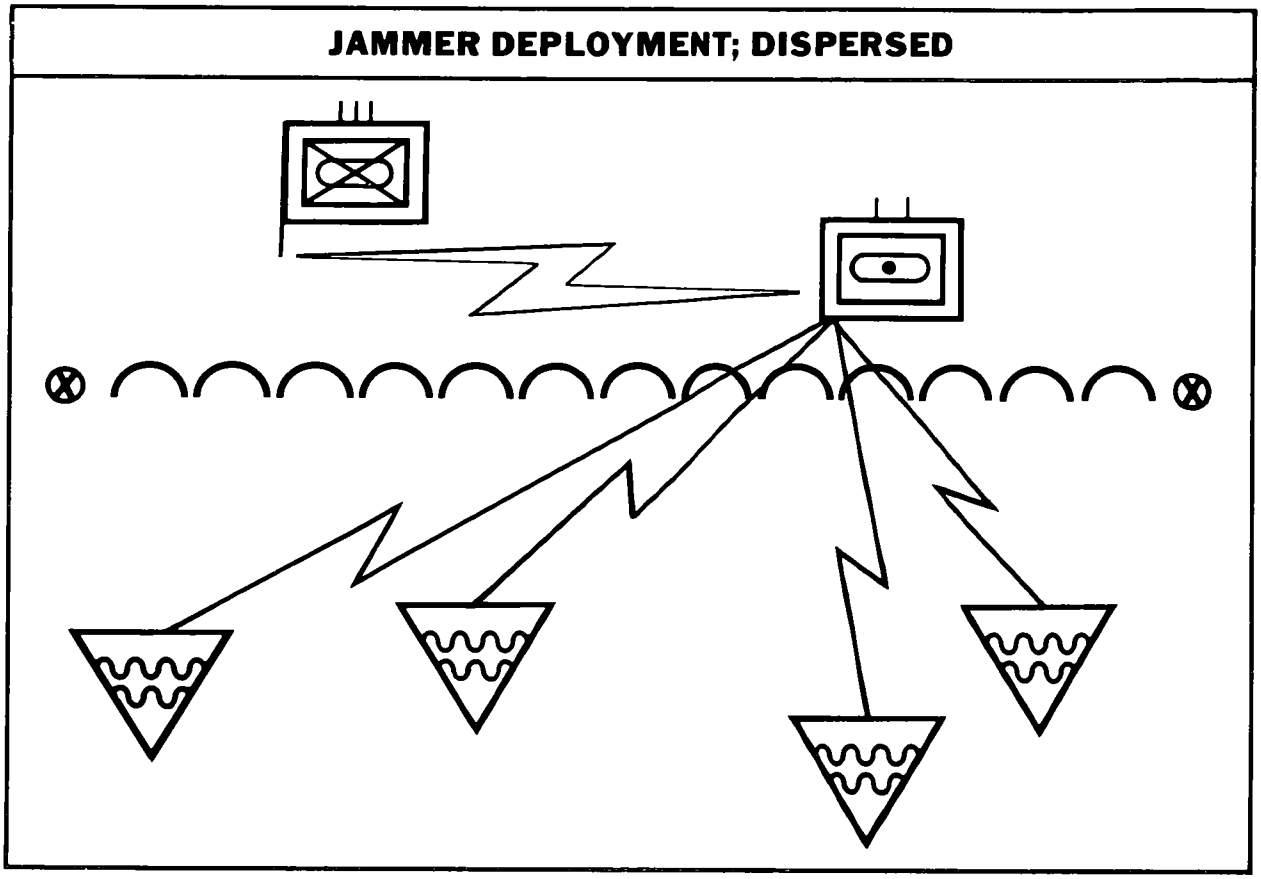
Deployment

Jammers are HPTs for destruction. Because of their high power output and unique electronic signature, they are relatively easy to detect and locate. Ground based jammers must deploy within range of enemy indirect fire weapons and their thin skin makes them highly susceptible to damage. Taken together, these factors dictate that jammer deployment be well planned and executed. Proper site selection and strict adherence to SOP are essential to survival.

General site locations are established by MI commanders or the TCAE, coordinated with the unit in whose area they are operating, and refined by the platoon or team leaders. Distance to the targeted enemy radio receivers, terrain, LOS, and the tactical situation are critical selection factors. Because of LOS requirements of VHF frequencies, jammers in that frecuency range will have to be close to the FLOT to accomplish the mission, probably within 2 kilometers. Where higher terrain is available, VHF jammers may successfully operate farther back. HF jammers may be as close as 7 kilometers but are usually farther back.

Jammers have to move to survive and to maintain favorable transmission paths against enemy radios which are moving as the battle progresses. Changes in battle lines will require frequent displacement. Primary and alternate sites are preselected for each phase of the battle. These sites must—

- ☐ Be accessible and concealed from enemy direct fire weapons.
- ☐ Provide for continuity of operations.



- ☐ Facilitate electronic massing of several jammers against single targets as shown in the illustration.
- ☐ Facilitate communications.

EXJAMs are used to overcome the LOS and distance limitations of standoff systems. EXJAMs can be hand-emplaced or artillery-delivered to target enemy receivers in a particular area. EXJAMs may also be mounted on unmanned aerial vehicles. Their proximity to target receivers enables them to effectively jam enemy communications with minimum interference to friendly systems. They are normally employed in an array to disrupt communications over a large area. EXJAMs are generally capable of barrage jamming.

Communications

Control and coordination are essential to effective EW operations. Communications is the key to effective control. Secure, reliable communications are required for—

- ☐ Tasking and technical support.
- ☐ Control of jamming operations.
- ☐ Tipoff and cuing between collectors and jammers, both air and ground, to include DF.
- ☐ Coordination between jammers.
- ☐ Dissemination of combat information.
- ☐ Resource status reporting.
- ☐ Mission status reporting.

Control Mechanisms

Control of jamming operations is essential to their success. Control keeps jamming directed at HPTs while minimizing its

effects on friendly systems and operations. Either positive or negative control methods may be used. However, a combination of both is generally used for maximum coordination between the ECM teams and the command they are supporting.

Positive control methods include—

- Authorizing specific frequencies for jamming on an individual basis or by publishing a list of frequencies cleared for jamming. No other frequencies may be jammed without permission.
- Authorizing specific enemy functions to be jammed unless they operate on a TABOO frequency.
- On-off control, which allows for the immediate starting or stopping of jamming. Reliable communications are required and the command's ability to exercise this type of control must be verified prior to its implementation. On-off control usually is exercised by the TCAE but may be held by the G3 or delegated to lower echelons as circumstances dictate. It is the most centralized form of control.

Negative control is exercised through the publication of frequencies restricted from jamming. These lists coordinate the use of the electromagnetic spectrum to impose a minimum of restriction on jamming or frequency usage. They are grouped into TABOO, PROTECTED, and GUARDED classifications. Conflicts in frequency grouping among services, staffs, and agencies are resolved at command level. Frequencies not on these lists may be jammed at will.

TABOO frequencies must never be deliberately jammed or interfered with by friendly forces. These frequencies are normally announced by higher headquarters such as the joint force or Army component commander. Examples include but are not limited to Defense Communications System (DCS) radar frequencies used for friendly early warning air defense, enemy frequencies being exploited by higher headquarters for intelligence purposes, frequencies used for C^2 of friendly forces and formations, friendly missile control frequencies, and search and rescue nets. TABOO frequencies also include internationally controlled or treaty-governed frequencies, such as broadcast emergency frequencies and commerical air and shipping traffic control frequencies. A TABOO frequency can be time-oriented, and the restriction may be removed as the situation develops. This decision is the responsibility of the originating headquarters. The G3, assisted by the C-E officer, is responsible for obtaining the TABOO list from higher headquarters.

PROTECTED frequencies are those used by tactical friendly forces for a particular operational requirement. They are designated by the senior tactical commander to control interference produced by friendly jamming and deception operations. Conflicts between frequency requirements for jamming and tactical command are resolved by the commander. The G3, assisted by the C-E officer, is responsible for obtaining the protected list of the next higher headquarters and adding local requirements.

GUARDED frequencies are those of the enemy's C-E systems from which SIGINT and ESM information of technical and tactical importance is derived. A GUARDED frequency may be jammed only after the commander has weighed the potential operational gain against the loss of information. The TCAE recommends GUARDED frequencies for approval by the G3 in coordination with the G2. These frequencies are time-oriented in that the list may change as the enemy assumes different combat postures.

ESTIMATE

Based on the commander's guidance, the G3 staff and the EWS prepare the EW estimate. The staff may issue initial warning orders to subordinate units to give them advance warning of a forthcoming action or order. This allows subordinates to forecast and state their EW support requirements. These may later form the basis for task organization of EW resources or affect the selection of a course of action.

IPB products are the basic tools for assessing enemy capabilities and vulnerabilities. They provide OB data and the probable disposition of forces and emitters.

Critical events are forecast by time and location which aids in identifying HVTs and determining the impact EW can have on the enemy. Terrain and LOS overlays together with friendly force information aid in determining EW resource deployment and estimating their effectiveness. Once planning is underway, the EW estimate is prepared.

The EW estimate is a logical presentation of enemy and friendly EW capabilities and vulnerabilities as they relate to the mission. It includes EW courses of action available to the commander and weighs the relative merits of each. Based on an analysis of all factors, the best EW course of action is recommended. The format of the EW estimate is given in Appendix D.

ANNEX

The EW annex details the EW mission, concept, and tasks to be performed by elements of the force. It describes how EW will be used to support the operation. It is prepared in the standard five-paragraph OPORD format by the G3 with major inputs from the G2, EWS, and C-E officer. For clarity and brevity, amplifying details are contained in appendixes to the annex. Electronic deception and defensive EW may be covered briefly in the EW annex with reference to the deception and C-E annexes when appropriate.

The appendixes to the EW annex provide the details necessary for subordinates to implement the plan. They may include a composite EW target list (at division level) and initial restricted frequency lists. These lists require periodic update during operations. These updates are normally disseminated informally rather than by republishing the EW annex.

ELECTRONIC WARFARE TASKING

Organic and supporting MI units are tasked to accomplish the ESM, communications, jamming, and IED missions stated in the OPORD. ESM requirements to support EW are developed by the G3 and EWS and stated to the G2. They are incorporated into the collection plan by the CM&D section and tasked as described in Chapter 3. The following illustration depicts the EW units organic to each tactical echelon.

Jamming and IED mission tasking is formulated by the EWS and transmitted to the MI tactical unit operations center. The TCAE allocates specific EW assets and tasks them to carry out the missions. This asset tasking contains the necessary technical and parametric data as well as the target, timing, priority, and control information provided in mission tasking.

ELECTRONIC WARFARE ASSESSMENT

As with any combat operation, the effectiveness of EW operations must be continuously evaluated. If the desired effect was not achieved, the reasons must be determined. Reevaluation of the target may lead to allocation of additional jamming resources, or it may be determined that attack by fire is preferred. If failure results from insufficient or erroneous information, ESM requirements are revised to make sure that information shortfalls are eliminated.

Assessment is crucial to the EW process. It identifies strengths and weaknesses and provides a base of knowledge for planning and executing future operations. Assessment is conducted at each step of the EW process to ensure that EW operations are responsive to the commander's need.

Both the TCAE and the EWS are involved in the assessment process. The TCAE is primarily concerned with assessing technical effectiveness while the EWS is more concerned with the overall effects on the enemy. Poststrike assessment was described in Chapter 3.

ELECTRONIC WARFARE UNITS			
ECHELON	MI ORGANIZATION	MAJOR EW UNIT	EW SUBUNIT
CORPS	BRIGADE	MI BN (TE) MI BN (TE) (RC) MI BN (AE)	EW CO EW CO (COLL) & EW CO (ECM) EW AVN CO
HEAVY DIV	BATTALION	C&J CO EW CO OPCON	C&J PLT (3) SIGINT PROC PLT QUICKFIX FLT PLT
LIGHT DIV	BATTALION	COLL CO OPCON	VOICE COLL PLT (3) QUICKFIX FLT PLT
AIR ASSAULT DIV	BATTALION	HHOC C&J CO	QUICKFIX FLT PLT C&J PLT (3) & NONCOM PLT
AIRBORNE DIV	BATTALION	C&J CO OPCON	C&J PLT (3) & NONCOM PLT QUICKFIX FLT PLT
ACR	COMPANY	—— OPCON	C&J PLT (2) QUICKFIX FLT PLT
SEP BDE	COMPANY		COLL PLT (VOICE) VHF ECM PLT

CHAPTER 6

Organization For Combat

IEW operations support combat operations. Given a mission by the force commander, the MI commander, subordinate commanders, and staffs must quickly determine the—

- Mission to be accomplished.
- Unit(s) to be supported.
- MI assets available.
- Organization of MI assets to provide the required support.

This chapter describes the principles that guide the MI commander and staff in organizing to meet IEW mission requirements. It describes command and support relationships and offers methods of task organizing an MI unit. It also describes the communications that are vital in organizing the MI unit for combat and ensuring the timely flow of information and intelligence which affects the outcome of the air-land battle.

COMMAND AND SUPPORT RELATIONSHIPS

The MI commander provides the direction to subordinate elements to accomplish the IEW mission generated by the force commander's concept of the operation. MI commanders command and control MI resources assigned to support the combat force. The command relationships which direct MI commanders are—

- Organic. Those assets which form an integral part of a military organization. These assets are listed in a TOE and specify the personnel, materiel, and structuring of a unit.
- Assigned. A unit which is placed in an organization on a relatively permanent basis and is controlled and administered for its primary function, or a greater part of its function, by the organization to which it is assigned.
- Attached. Attachment places a unit under the temporary C^3 of another unit. The directive establishing this relationship establishes specific terms of attachment, such as the provision of CSS. Although subject to limitations specified in the attachment order, the commander to which the unit is attached exercises the same degree of C^2 over the attached unit as over those units ogranic to the command.
- Operational control. This relationship places one unit under the control of another for its direction and employment. OPCON basically has the same intent as attachment but the controlling unit does not have responsibility for logistical and administrative support. OPCON does not permit the gaining commander to tailor the unit placed under OPCON.

During IEW operations, MI assets are assigned standard tactical missions. Standard missions describe in detail the IEW support responsibilities for an MI unit. They also establish an MI unit's relationship to a supported force or another MI unit. Standard tactical missions do not affect the organizational structure or the command relationship that results from that structure.

The four standard tactical missions are—

- DS.
- GS.
- Reinforcing.
- General support reinforcing.

An MI element in DS of a specific unit is required to respond to the IEW requirements of that unit. The supported unit will identify its requirements through liaison elements, which will route them to the MI element for execution. As well as their first priority to respond to the requirements of the specified unit, DS elements have a

second priority to respond to the needs of the force as a whole. A unit in DS has no command relationship with the supported unit, and remains under the C^2 of its MI chain of command.

An MI element in GS will provide support to the force as a whole and not to any particular subordinate unit. It responds to the requirements of the force commander, as tasked by the MI unit TOC.

The IEW capabilities of MI units or staff sections are extended by MI units reinforcing other MI units. Reinforcing MI units remain under the command of the MI commander assigning the reinforcing mission, while operational control is retained by the MI unit or staff sections being reinforced. The reinforcing mission permits increased support to specific maneuver units without giving up complete control of MI assets to the supported elements.

An MI element assigned a general support reinforcing mission is required to respond first to the IEW requirements of the force as a whole and then to reinforce the activities of another specified MI element as a second priority. The general support reinforcing mission gives the force commander the flexibility needed to meet the changing tactical situation.

There are inherent responsibilities within each standard mission. The following matrix illustrates these responsibilities as applied to the four standard IEW missions.

PRINCIPLES OF ORGANIZATION

All actions in the air-land battle are based on the nine principles of war. These principles are fundamental, interrelated concepts that vary with the situation. In organizing for combat, four of the nine principles take precedence for consideration by MI commanders. They include—

- ☐ Objective.
- ☐ Economy of force.
- ☐ Unity of command.
- ☐ Simplicity.

MI commanders must understand clearly the overall mission of the force commander, the MI unit mission, and how the MI unit will be organized to support the force commander's objective. They select objectives for MI unit assets that will directly and indirectly contribute to the ultimate objective.

The principle of economy of force requires that MI commanders organize limited available MI resources with emphasis in the area where the main effort of the force will take place. However, MI commanders must also allocate resources that will adequately support secondary efforts.

MI commanders ensure unity of command by coordinating the actions and organization of all MI assets toward the common goal through mission orders. MI commanders control their subordinates, yet extend to them the freedom to exercise their initiative.

MI commanders accomplish the mission in the simplest way possible. Direct, simple plans and clear, concise orders reduce misunderstanding and confusion. Simplicity generates flexibility and results in responsive IEW support.

TASK ORGANIZATION

MI units organize for combat to provide the best possible mix of MI assets to support the force commander's concept of operation. The MI commander must retain ***flexibility*** by organizing the unit to quickly adjust to the unexpected. Flexibility is achieved by planning for each possible contingency. This requires MI commanders and staffs to identify MI assets from one or more units that can be task organized rapidly and moved to a designated location on the battlefield. Flexibility also eliminates the need for establishing IEW reserve forces.

STANDARD TACTICAL MISSION RESPONSIBILITIES MATRIX

AN MI UNIT WITH MISSION OF... RESPONSIBILITY	DIRECT SUPPORT	REINFORCING	GENERAL SUPPORT REINFORCING	GENERAL SUPPORT
Responds to requirements of	1. Supported unit 2. Force as a whole	Reinforced MI unit	1. Force as a whole 2. Reinforced MI unit	Force as a whole
Technical control	MI Bn TOC	1. Reinforced MI unit 2. MI Bn TOC	1. MI Bn TOC 2. Reinforced MI unit	MI Bn TOC
Zone of action	1. Supported unit area of opns 2. Div area of opns	Same as reinforced MI unit	1. Div area of opns 2. Same as Sup units	Div area of opns
Furnishes IEWSE	MI battalion (division) provides an IEWSE to each maneuver brigade regardless of what MI assets are in the brigade AO.			
Establishes comm with	1. Supported unit 2. MI Bn TOC	1. MI Bn TOC 2. Reinforced MI unit	1. Reinforced MI unit 2. MI Bn TOC	MI Bn TOC
Is positioned by	MI Unit Commander in coord w/ supported unit	Reinforced MI unit or as ordered by MI Bn TOC	MI Bn TOC or reinforced MI unit if approved by MI Bn TOC	MI Bn TOC
Tasked by	1. Supported unit 2. MI Bn TOC	Reinforced MI unit	1. MI Bn TOC 2. Reinforced MI unit	MI Bn TOC

In organizing for combat, MI commanders assign resources to support the force commander's battle. In allocating MI assets for DS and reinforcement, consideration must be given to retaining sufficient assets in GS and general support reinforcing roles to provide the flexibility to influence the battle at critical times and places. Considerations which the MI commander must make when organizing for combat are—

- Degree of control.
- Sufficient support to accomplish the assigned mission.
- Future operations.

MI units require a sufficient degree of centralized control to maximize their capabilities to influence close and deep operations. Each tactical mission requires a different degree of centralized control which will affect MI responsiveness to supported forces. In the defense, more centralized control allows the force commander to influence close operations as it develops and at the same time concentrate on deep operations. In the offense, a moderate degree of centralized control allows subordinate MI commanders and leaders the initiative to develop the tactical situation and provide the supported tactical commander the information needed to exploit opportunities and maintain momentum.

Sufficient support is provided to the force commander by assigning standard IEW missions. MI units are most responsive to a supported commander in the DS role. Additional support is provided with other MI units in reinforcing or general support reinforcing roles. In the offense, the sector of the main attack should be weighted with the required MI assets. In the defense, MI assets are weighted to the covering force first and then to the most probable enemy avenue of approach. Weighting is accomplished by—

- Stating priority of IEW effort to forward deployed force.
- Assigning reinforcing or general support reinforcing missions to some IEW assets which provide immediate response to the IEW assets supporting forces in contact. This increases the IEW support in a specific area to respond to the needs of a commander.
- Positioning of GS assets and assigning those assets an area of coverage that concentrates on a critical sector or zone of the battlefield.

MI commanders must assure uninterrupted IEW support by organizing their units in such a way as to ensure the smooth transition from current to future operations. The MI commander does not hold assets in reserve. Immediate responsiveness to the force commander's priorities demands that the MI commander organize MI units with a mix of assets that provide multidisciplined support to the maneuver force. Future operations are facilitated by—

- Using on-order missions.
- Providing a comprehensive CSS package.
- Dispersion of units to provide survivability from chemical and nuclear attacks.
- Detailed SOPs that provide flexibility.

MI resources are organized for combat to provide the most reliable and responsive support possible to the combined arms team. Each level of command—MI company through MI brigade—organizes according to the mission and the resources available. How a particular unit is organized depends on METT-T.

Through the distribution of assets, the MI commander rapidly organizes for combat and readjusts the organization as the tactical situation changes. Shifting assets between command structures creates a mix of MI assets immediately responsive to the force commander's maneuver plan.

Divisional MI battalion commanders must establish control measures for deployed MI assets. The degree of control required depends on the number and diversity of the MI resources operating in a given area. When sufficient numbers are deployed, IEW company teams are formed to provide the required control. In addition to the operational elements, maintenance elements deployed and operating in the area are included in the company team.

THERE IS NO STANDARD ORGANIZATION FOR AN IEW COMPANY TEAM. THE FORMATION AND ORGANIZATION OF EACH COMPANY TEAM IS DEPENDENT SOLELY UPON THE RESOURCES OPERATING IN A GIVEN AREA AT ANY GIVEN TIME.

The following illustration depicts one method of organizing a company team based on the MI assets operating in a brigade area. A detailed description of IEW company teams and their control is provided in Chapter 3, FM 34-10.

The MI brigade commander (corps) has less flexibility when organizing for combat since the MI brigade principally provides GS to the corps. Aerial assets, such as GUARDRAIL and QUICKLOOK, remain as a battalion at corps. Depending on the tactical situation, these may weight support to one of the divisions, or the ACR. MI elements from the MI battalion (TE) (EW, interrogation, and CI elements) are normally organized as platoons or teams and assigned corps GS missions or attached to the MI units at division or ACR. FM 34-25 describes how an MI brigade organizes for combat.

MI company commanders in support of ACR or separate brigade deploy and fight assigned IEW assets of the company, with the exception of GSRs, under control of the MI company. The role of the MI company in support of the ACR operations is described in FM 34-35.

COMMUNICATIONS

Every aspect of IEW operations is dominated by the requirement for rapid, reliable, redundant, and secure communications. IEW assets cannot perform the mission for which organized unless they can be effectively tasked and controlled. In addition, the value of information they collect is questionable unless it is rapidly transmitted to the processing and combat elements needing it.

The communications needed for C^2, administrative and logistical actions, and intelligence and combat information reporting are the basis for development of communications systems and nets.

Combat information and intelligence are critical to the conduct of tactical operations. When possible, combat information must flow directly from the collector or processor to the user. Intelligence and targeting data must be communicated quickly to users or processing elements. Communications for administrative and logistical operations are essential to sustain IEW personnel, equipment, maintenance, and supply. Communications means must support information exchange between coordinating staffs, supporting CSS units, and MI units and subordinate elements.

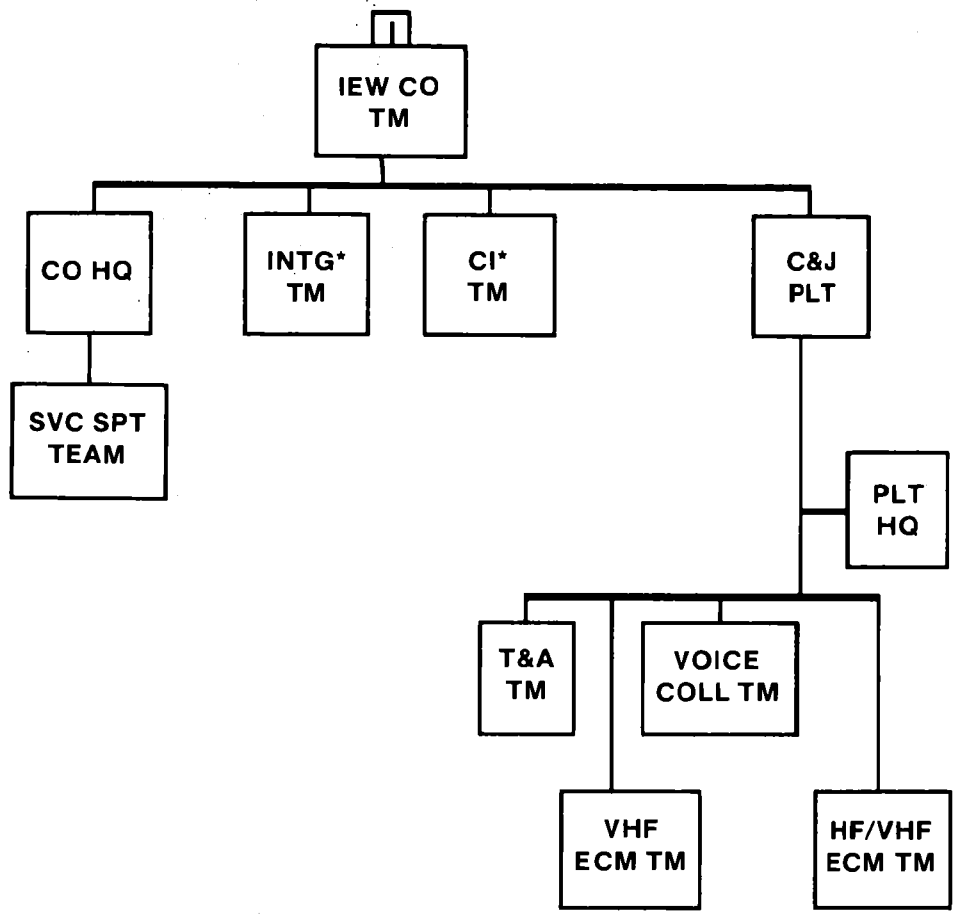
MI units use several types of communications to ensure the efficient flow of information. These are—

- The multichannel system.
- RATT.
- FM voice radio (secure).
- Landline telephone.
- Radio-wire integration.
- Messenger or courier.
- Facsimile

RATT communications are the primary means for record traffic used for tasking and reporting.

Multichannel systems (or links) provide communications for combat operations and tie units into the area communications system. Multichannel systems are the backbone of the division, corps, and EAC communications system. Terminal equipment,

A TYPE IEW COMPANY TEAM



* WHEN SUFFICIENT AUGMENTATION IS RECEIVED FROM CORPS

required for multichannel communications, is installed and maintained by the signal units. Current intelligence requirements for direct, high security communications links are met by the multichannel system. Automated switching systems meet the requirement for both speed and security. MI units at corps and division use the multichannel system for much of their communications needs. As it is a common-user system it provides for communications from widely dispersed MI assets to their MI unit TOC or the DTOC or CTOC. For example, interrogators at the division's main EPW cage will use the nearest terminal of this common-user system to report results of interrogation and screening to the CM&D at the DTOC.

FM voice radio is the primary means of communications for command and control, administrative, and logistical information. At division and ACR, FM radio is often the only means of tasking and reporting between specific MI elements.

Wire is one of most dependable means of communications available to MI elements. The MI commander's decision to establish landline communications must be based on need, time available, and the ability to maintain it. The best use of landline is to interconnect closely located activities, such as CPs and operations centers, that remain relatively stable.

Net-radio interface (NRI) is flexible, responsive, and provides the MI commander with additional communications means. Responsibility for providing NRI facilities belongs to supporting signal elements; however, the transmitter link to the NRI facility is the responsibility of the supported MI unit.

Messengers or couriers provide a secure means of delivery for large or bulky items such as map overlays or large quantities of message traffic. Strong consideration should be given to the use of messengers or couriers in and around TOCs and other closely located activities. Care must be taken to ensure that classified information is entrusted to only those couriers cleared for the level of material in their possession.

Coordination of IEW activities between corps, divisions, and ACRs is through CM&D-to-CM&D and TCAE-to-TCAE communications. The MI brigade provides the dedicated RATT communications required for this purpose.

EAC is responsible for dedicated communications between the echelon above corps intelligence center (EACIC) and corps ASPS. Intelligence and targeting data are disseminated to and received from other services and allies through the EACIC located at the joint intelligence center (JIC). Information from the national level is disseminated directly to the corps and the JIC simultaneously. The following matrix identifies the principal stations and means of communications for IEW operations.

This matrix identifies the principal stations and means of communications used for tactical IEW operations, tasking, and reporting. Not all stations have been identified. Dissemination channels are not shown. Reliance upon intelligence nets at each level of command, direct dissemination channels established as required, and staff interfaces satisfy dissemination communications requirements.

Each tactical echelon of command normally operates an operations and intelligence net. Controlled by the G3 or S3, this net links major elements of the command for the reporting and dissemination of orders, intelligence, and combat information. MI unit TOCs are stations in these operations and intelligence nets. Operations and intelligence nets are normally FM (secure). A standby courier capability should be established at each echelon of command as backup, and for the transmission of bulk products to enhance COMSEC.

PRINCIPAL TASKING AND REPORTING COMMUNICATIONS

	EACIC	CTOC CM&D SEC	MI BDE TOC/TCAE	DTOC CM&D SEC	MI BN TOC/TCAE	ACR TOC SPT PLT	SEP BDE TOC SPT PLT	BDE IEW SPT ELE
CTOC SPT ELM (CM&D SEC)	□ •		□	□[1] •		□ •	□ •	
MI BDE TAC OP CTR/TCAE		□ •			□ •	□ •		
DTOC SPT ELE (CM&D SEC)		□[1] •			X □			
MI BN TAC OP CTR/TCAE			□ •	• X				X
ACR TOC SPT PLT		□ •	□ •					
AVN CO (AS) (MI BN (AE))		□ •	• X □					
AVN CO (EW) (MI BN (AE))			□ •					
ECM & INTCPT PLTS (MI BN (TE))			•					
CI INTG CO (MI BN (TE))		□ •	X					
CI/EPW TEAMS (DIV)				□[2]	X			
C&J PLT (DIV)					X			X
BDE IEW SPT ELM					X			
SIGINT PROC PLT (DIV)					•			
CEWI FLT PLT (DIV)					X			
SURVL PLT (DIV)								
OPS SPT PLT (ACR) (SEP BDE)						X	X	
C&J PLT (ACR) (SEP BDE)						• X	• X	
SURVL PLT (ACR) (SEP BDE)						X	X	
CEWI FLT PLT (ACR)						X	X	
CORPS TAC CP		• X						
DIV TAC CP				X △	X			

□ - MULTICHANNEL

• - RADIO TELETYPEWRITER

X - FM RADIO

[1] CM&D TO CM&D COMMUNICATIONS INCLUDE SSO AND WEATHER COMMUNICATIONS

[2] REPORTING ONLY

CHAPTER 7

Offensive Operations

Successful offensive operations demand imagination, thorough coordination, and skilled execution. They are characterized by aggressiveness, initiative, rapid shifts in the main effort to take advantage of opportunities, momentum, and deep, rapid destruction of enemy forces. Offensives should move fast, follow successful probes through gaps in enemy defenses, and shift strength quickly to widen penetrations and reinforce successes to carry the battle deep into the enemy's rear. They should destroy or control the forces or areas critical to the enemy's overall defensive organization before the enemy can react.

Offensive operations are undertaken primarily to destroy enemy forces. They may also—

- ☐ Secure key terrain.
- ☐ Gain information.
- ☐ Deceive and divert the enemy.
- ☐ Deprive the enemy of resources.
- ☐ Fix the enemy in position.

Secondary purposes contribute to the destruction of enemy forces, but are almost never ends in themselves.

The destruction of the enemy fighting force and its will to resist is the only way of winning in combat. Doing so is most practical after the enemy has been driven from prepared positions or caught in a vulnerable position. This purpose is well served by effective and efficient IEW support.

IEW PRINCIPLES

In the offense, certain IEW principles are essential to battlefield success:

- ☐ Knowing the battlefield.
- ☐ Denying the enemy intelligence.
- ☐ Disrupting and destroying enemy command, control, communications, and intelligence (C^3I).
- ☐ Maintaining the integrity of IEW operations.

KNOWING THE BATTLEFIELD

Offensive operations require detailed intelligence on the enemy, weather, and terrain. Detailed, accurate, and comprehensive IPB begins before initial deployment and continues during the battle. Knowing the battlefield, commanders can attack over advantageous terrain. They can use terrain for masking and seize key terrain. They can exploit weaknesses in the way the enemy uses terrain.

To avoid a tactical surprise, the commander must locate enemy forces, including defensive units and reserves, as early as possible. To prevent surprise and to estimate enemy intentions, the commander places the battlefield under continuous surveillance in depth. Commanders rely heavily on aerial assets to see deep. Armored cavalry squadrons, because of their mobility and organization can perform security and reconnaissance operations over large areas.

Once the enemy force is located, IEW assets track its movement continuously for both intelligence and targeting purposes. IEW assets monitor HVT, track enemy forces, and pass essential information to the targeting cells. Ground intelligence assets provide mobile support to the developing close operations, using leapfrog movement. MI must collect information which will reduce the friendly commander's uncertainty about the battlefield.

Offensive operations pit friendly strengths against enemy weaknesses. Therefore, MI systems determine enemy vulnerabilities which friendly commanders can exploit while simultaneously avoiding known enemy strengths.

IEW assets available to friendly commanders are limited and must be used judiciously. Centralized collection management is essential. All collection operations must support PIR and IR.

DENYING THE ENEMY INTELLIGENCE

IEW systems seek to reduce battlefield uncertainty for the friendly commander and increase uncertainty for the enemy commander. A primary element in doing so, CI—

- ☐ Monitors force OPSEC posture.
- ☐ Identifies and recommends measures to conceal friendly profiles.
- ☐ Monitors and recommends OPSEC measures.

Deception operations may be critical to denying the enemy accurate, clear information about friendly forces. Well planned and coordinated deception operations will increase the enemy's uncertainty of the battle area by misleading and confusing his intelligence system. Deception operations may include both electronic and tactical deception measures.

DESTROYING AND DISRUPTING ENEMY C^3I

MI units support the destruction and disruption of enemy C^3I systems through ECM. Timing ECM missions, to include electronic deception and selecting targets, is critical to gaining the maximum effect.

There is a significant CI mission on the battlefield, particularly in the rear area. CI assets not only support OPSEC but also isolate key targets of interest for exploitation or neutralization. Then, as the force moves forward into areas previously under enemy control, CI actively seeks out personnel engaged in espionage, sabotage, or subversion against US forces. Close coordination with higher echelons for CI target development is necessary.

MAINTAINING THE INTEGRITY OF OPERATIONS

The integrity of IEW operations is tied to the integrity of the force as a whole. In weighting the main attack at a particular place and time, the commander takes risks elsewhere. In these areas, mobile MI assets serve in an economy of force role to provide early warning and to support deception operations. MI assets supporting the main attack and those serving in an economy of force role must be task organized and tailored to suit the mission and mobility requirements of the force.

Survivability of IEW assets is essential in any operation and particularly so in offensive operations. Consistent with security and communications requirements and mission responsiveness, IEW assets should disperse to the maximum extent possible. They also apply the full range of OPSEC measures.

Command and control of IEW resources and their effectiveness are directly related. If IEW is to be continuous and responsive, the level, type, and means of command and control of these assets must be determined early.

SUPPORT TO THE OFFENSIVE

IEW elements provide support to all forms of offensive operations. The five primary types of offensive operations are—

- ☐ Movement to contact.
- ☐ Hasty attack.
- ☐ Deliberate attack.
- ☐ Exploitation.
- ☐ Pursuit.

These operations are described in detail in FM 100-5.

MOVEMENT TO CONTACT

Movement to contact is a tactical operation to find and engage the enemy. The force is organized to hold the bulk of its combat power in the main body. It moves aggressively toward the enemy, making maximum use of IEW resources to find the enemy before the enemy detects the friendly force. CI denies the enemy intelligence about the force. When contact is made, combat information and intelligence determine where and with what force to attack to overcome enemy resistance. ECM supports the attack.

In a movement to contact, the friendly force may encounter an enemy that is defending or moving to contact. Once contact is made, the action must be resolved quickly if the movement to contact operation is to continue. This is normally done by means of a hasty attack launched as quickly as possible with whatever assets are on hand. No time is available for detailed IPB and analysis, other than what was done prior to the beginning of the operation. The intelligence analysis is quickly updated for the commander and continues to be updated as the attack progresses. If the enemy is in a well-prepared defensive position and a deliberate attack is necessary, then detailed IPB and analysis is necessary to provide critical information about—

- Enemy defensive belts.
- Obstacles supporting the enemy's defensive plan.
- Enemy security forces.
- Enemy nuclear and chemical delivery means.
- The best avenues of approach into the defensive area.

Should the enemy force be in a march to contact formation, IEW resources provide critical information about—

- Enemy reconnaissance elements, advance guard (combat reconnaissance patrols, forward security element, the advance guard main body), the main force, the rear party, and flank security parties.
- Probable enemy courses of action and their effect on friendly courses of action.
- Flank security data.

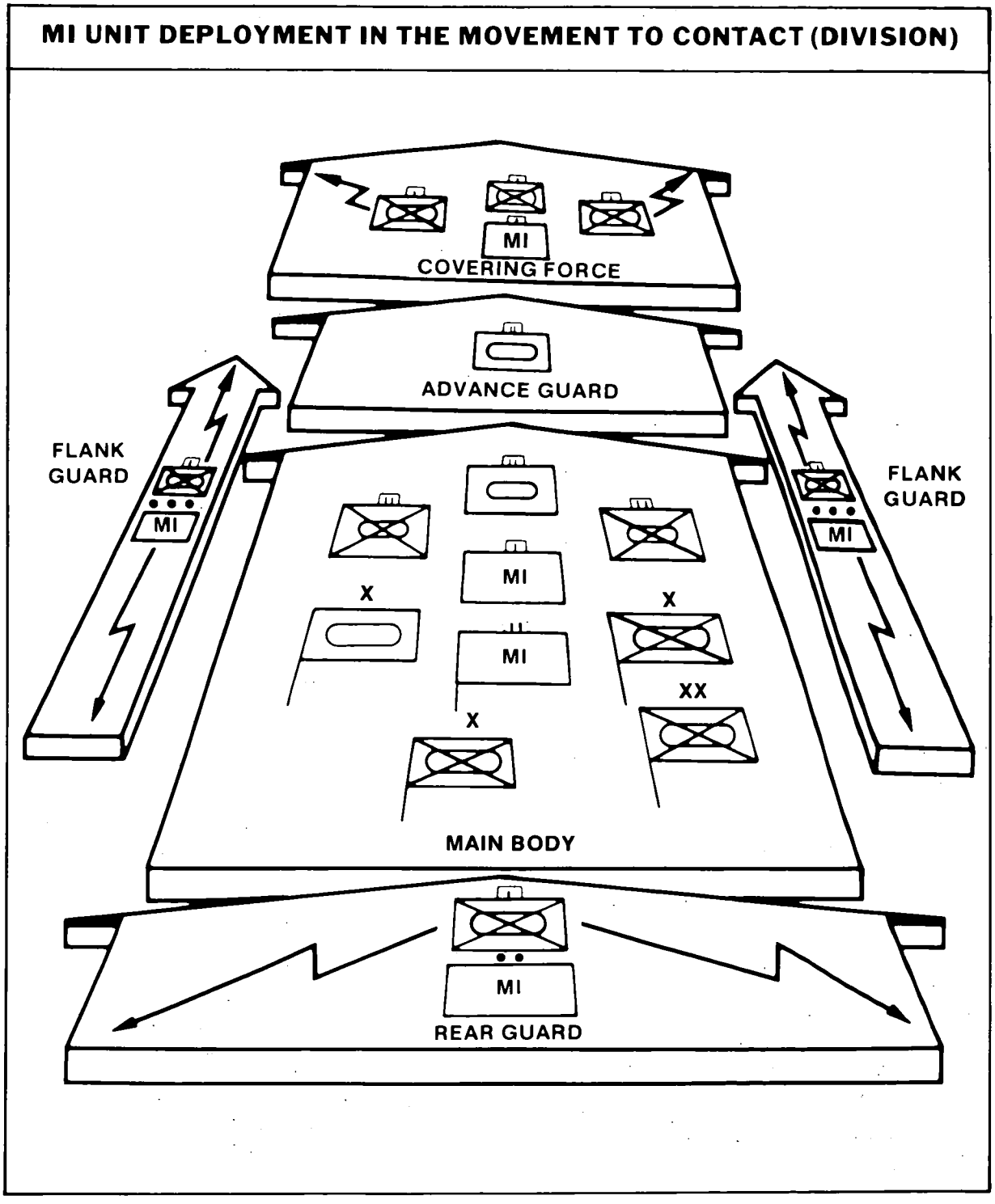
IEW resources look deep to determine second-echelon vulnerabilities. These vulnerabilities form the basis for friendly offensive action, particularly deep interdiction. Many of these vulnerabilities will be associated with HVTs—both natural and manmade. IEW resources identify, locate, and track HVTs and monitor selected key terrain.

While continuing to look deep, IEW resources also support close operations directly. They continue to be sensitive to enemy vulnerabilities which would bring maximum friendly success when exploited. Where possible, IEW resources support deception operations.

Interrogators deploy well forward to interrogate indigenous personnel, particularly refugees, to determine as much as possible about the enemy and terrain which lies in the path of the advancing force. GSR teams also deploy forward and on the flanks of lead elements to provide early warning and flank security to the force. To provide responsive support, ground-based ESM and ECM assets deploy as far forward as security and the mission allow. These assets use leapfrog movement techniques in order to provide support as continuously as possible. Aerial EW assets cover the times when ground assets are moving or are masked by terrain. They are also tasked to look deep, beyond the range of ground-based systems. CI teams work closely with interrogators in screening local nationals about the situation in front of friendly forces. They also implement CI plans prepared prior to the movement to contact by neutralizing or safeguarding persons identified on white, black, or gray lists.

MI assets are deployed to directly support forward deployed elements. This ensures the most responsive IEW support possible to forces leading the movement to contact. MI assets designated to support deep operations require much more centralized control in order to derive maximum effectiveness for the force as a whole.

The following illustration depicts a unit in the movement to contact formation with typically deployed MI assets.



MEETING ENGAGEMENT

The meeting engagement may be the end result of a movement to contact. It occurs when a moving force, incompletely deployed for battle, engages an enemy force about which it has inadequate intelligence. Once contact is made, ECM are employed against key C^2 communications and electronic guidance systems. All available collection resources deploy to determine the size, composition, disposition, capabilities, and intentions of the enemy force. They immediately report critical information, such as the location of assailable flanks and other enemy vulnerabilities, to the force commander. The commander needs such information quickly to decide whether to bypass, attack, or defend against the enemy. Effective integration and use of IEW resources generally preclude meeting engagement battles. If intelligence is effective, the commander can prepare for battle before encountering the enemy force.

HASTY ATTACK

Hasty attacks are launched with minimum advance warning or planning. They usually develop from movement to contact, but commanders can also use them to seize the initiative following a successful defense. At company level and below, hasty attacks are often launched using battle drill. Battalions employ preconceived plans to launch hasty attacks. Brigades and divisions improvise hasty attacks or conduct them by executing contingency plans.

DELIBERATE ATTACK

Deliberate attacks employed against a prepared enemy are thoroughly planned and coordinated and take time to prepare. In a deliberate attack, the commander trades momentum and possibly the initiative for the time required to assemble additional resources, including IEW resources, for the attack. Sufficient information must be available to plan the attack properly and synchronize all elements of the force.

MI support to the maneuver commander is critical as his forces consolidate on an objective. This is the time when he is most vulnerable to counterattack either by maneuver or fire. At objective consolidation, MI assets must be positioned to provide immediate support and facilitate early warning of such a counterattack.

In both the hasty and deliberate attacks, IEW tasks are virtually the same. MI resources determine as much information as possible about the enemy's defensive posture. Key information determined by IEW assets includes—

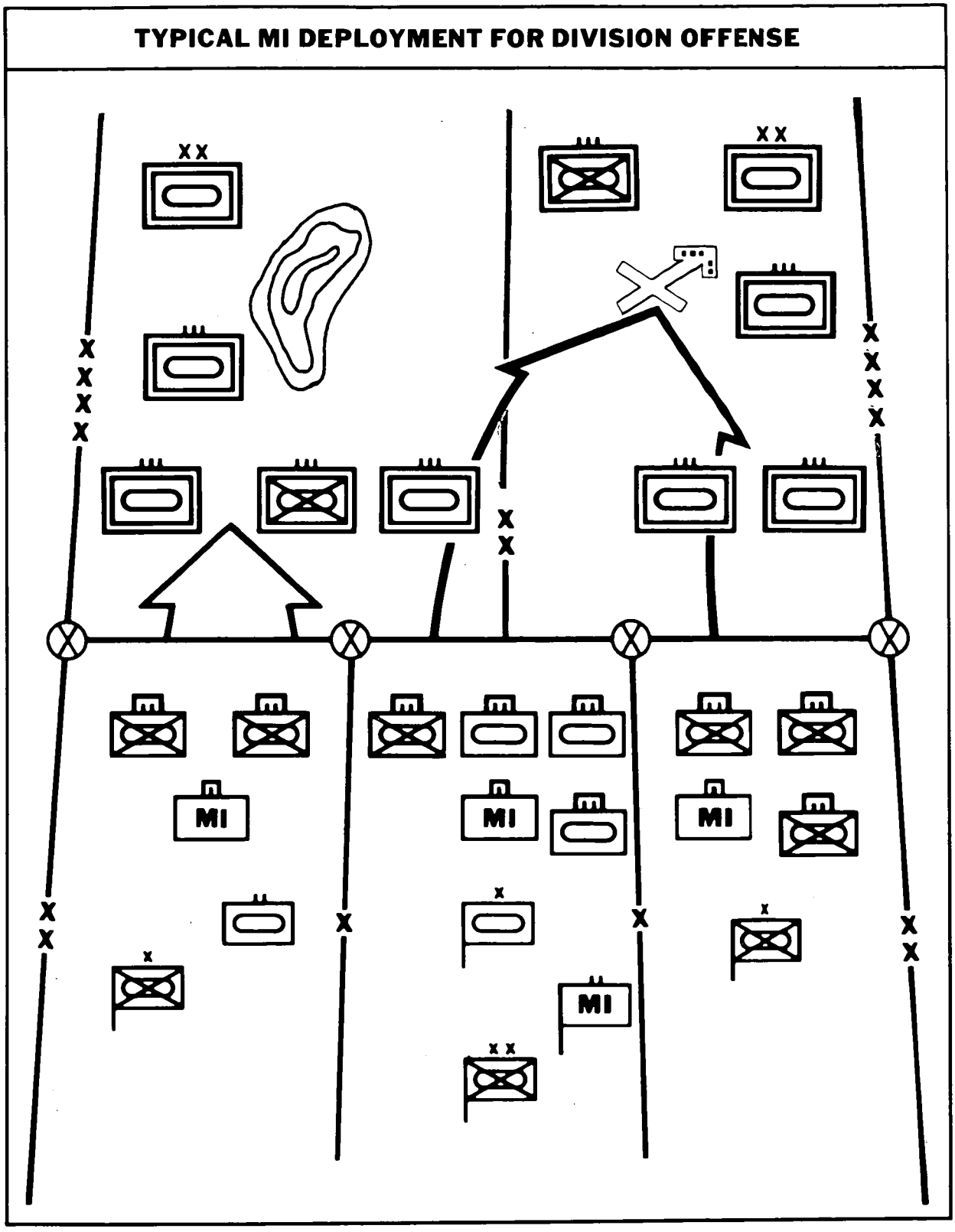
- ☐ How the enemy's defense is organized.
- ☐ Where enemy reserve and counterattack forces are located and when they move.
- ☐ What NBC weapon systems the enemy has and where they are located.
- ☐ Where the enemy's conventional artillery is located.
- ☐ Where enemy REC assets are located.

MI units may deploy for the attack as shown in the following illustration.

IEW resources with either the main or supporting attacks are tailored to the particular mission and scheme of maneuver. MI units must be able to keep pace with attacking forces and still provide support. Certain MI elements cannot operate on the move; therefore, they must use leapfrog techniques. In highly mobile situations, aerial systems provide continuity of support while ground assets relocate to new positions.

Fluid action will be common on the battlefield, and MI units must be tailored and employed for flexibility. When a supporting attack meets with unexpected success, the commander may elect to exploit it, making it the main effort. MI units must be prepared for this contingency. Should forces shift laterally across the battlefield to accomplish this objective, MI elements must be sufficiently mobile to keep up with them.

TYPICAL MI DEPLOYMENT FOR DIVISION OFFENSE



EXPLOITATION AND PURSUIT

Commanders planning offensive operations must be prepared to conduct exploitation and pursuit actions. Without prior detailed planning for these contingencies, fleeting opportunities to press a successful attack to completion may be missed. IEW resources, particularly MI assets, play an important part in planning for and executing exploitation and pursuit missions.

IPB is critical and helps identify enemy vulnerabilities. Intelligence supports targeting by identifying, locating, and tracking enemy forces which may move to counter exploitation forces.

Following the initial assault, MI units determine the integrity of the enemy's defense. They locate gaps, holes, and weak spots that may be exploited. They determine if the enemy intends to defend in place, delay, or withdraw to subsequent defensive positions. ECM are maximized to increase enemy force confusion. MI units continually pass intelligence on the withdrawing force's direction and rate of movement, locate and track HVTs, and provide targeting data to FSEs. They identify exposed or open enemy flanks which are vulnerable to offensive action.

To prosecute the exploitation and pursuit successfully, commanders apply pressure against the enemy continuously. Its most vulnerable areas are located, identified, and targeted. Such targets include communications, supply, and maintenance centers in the rear areas. As the force drives forward, these targets become increasingly vulnerable to friendly action.

As the offensive continues, two events will occur. First, the enemy will respond with strong, violent counterattacks. Aerial surveillance and reconnaissance assets look deep into second- and follow-on echelons to identify, locate, and track counterattacking forces. Intelligence and combat information about these forces is disseminated quickly to the commander, staff, and FSEs. Deep interdiction delays, disrupts, and destroys these forces so that exploitation can continue. MI assets remain alert to any attempts to outflank or cut off friendly forces which have driven deep into enemy territory. To prevent surprise, they keep the commander constantly informed.

Second, the enemy will probably reconstitute its defense. MI determines the place, time, and type of defense being established. They perform the same functions as described earlier in support of the deliberate attack.

ECM are critical in conducting exploitation and pursuit. Jamming is especially important. Jamming selected key C^2 communications at decisive times enhances the combat power of the attacking force. ECM assets provide the most mobile support possible to pursuing forces. Aerial assets provide near-continuous support in highly mobile situations. Surveillance assets deploy well forward to provide early warning and on the flanks to provide force security.

As is the case with all IEW assets supporting this offensive maneuver, agility must be planned in advance. MI resources must be capable of shifting rapidly to meet the changing demands of the battlefield, especially on the extremely extended flanks of deep penetrations.

CI supports the whole force. Although the ability to perform detailed analysis or to recommend countermeasures is diminished because of the rapid pace, CI still plays a valuable role. Monitoring EEFI and taking measures to protect them are key tasks. The success of exploitation and pursuit operations is closely linked to their security.

RECONNAISSANCE IN FORCE

A reconnaissance in force is a limited-objective operation by a substantial force to obtain information and to determine enemy dispositions and strengths. The reconnaissance in force also tests enemy reactions to friendly force action. Enemy reactions may reveal major defensive weaknesses which could be exploited. Even when using it to gain information, commanders executing a reconnaissance in force must be alert to seize an opportunity to exploit tactical success. If the enemy situation must be developed across a broad front, a reconnaissance in force may probe the enemy at selected

points. Recognizing that reconnaissance in force is primarily an information gathering operation, commanders must carefully consider the risks involved. Precise plans must be made in advance to extricate the force or exploit success. Commanders must be prepared to develop the success initiated by the reconnaissance in force into a full-fledged offensive operation.

IEW principles for reconnaissance in force are the same as for any other offensive operation. Additionally, however, IEW resources, as well as the entire force, must be prepared to exploit enemy reactions.

In many respects, MI for the reconnaissance in force is much like that for the movement to contact. Supporting MI resources are tailored in such a way that, should the reconnaissance in force develop into another form of offensive maneuver, those resources would be able to continue to provide support. To accomplish this, only the most mobile ground assets support the reconnaissance in force. Maximum use is made of aerial assets to provide continuity of support.

MI support in a reconnaissance in force is decentralized to the extent possible to ensure timely support to the commander. This is because the reconnaissance in force can easily develop into a hasty attack. Supporting MI resources plan for on-order missions which may derive from the tactical situation.

Regardless of the specific type of offensive operation conducted, IEW resources are vital to the success of all offensive operations. Without sound intelligence upon which the commander can make tactical decisions with a degree of certainty, successful offensive operations are unlikely. Well-timed and well-planned EW operations also make a significant contribution to well-executed attacks. Finally, intelligence support to OPSEC is essential to the security of both the force and the operations it conducts.

RIVER CROSSING

River crossing operations are an integral part of land warfare. The objective of any river crossing operation is to project combat power across a water obstacle while ensuring the integrity and momentum of the force. Because the modern battlefield is so lethal and because even small enemy units can be destructive, crossings must be quick, undetected, and coherent. It is essential, therefore, that rivers be crossed in stride as a continuation of operations.

River crossing is a special operation because it requires more planning and support than normal operations. It also requires unique operational considerations. In this case, however, special does not mean an uncommon or infrequently conducted operation. In central Europe, for example, rivers, lakes, and canals greater than 18 meters wide occur on an average of every 50 kilometers. Thus, river crossing operations must be integral to all tactical operations and practiced regularly. River crossings are normally conducted by divisions but may be conducted by corps. Brigades and battalions may cross independently or as elements of a larger force. Regardless of size, MI units support all river crossing operations.

To succeed, river crossings require concentration of effort, speed of execution, flexibility, and audacity. Planning ensures that the correct type and mix of equipment and support arrive at the designated crossing site at the proper time.

Command and control of river crossing operations is the most difficult part of the operation. Centralized command of the operation ensures coordination of assault, MI, and other units. Positive control of crossing elements while concentrating, moving across, and dispersing increases the probability of success. However, the plan must be sufficiently flexible to permit adjustments and changes during execution.

A crossing force commander is designated to plan and control the operation. In a division crossing, the crossing force commander usually is the assistant division commander for maneuver. The crossing force commander is assisted by a crossing force staff which includes G2 and G3 elements. In addition to a crossing force commander, each crossing area has a crossing

area commander who is normally a brigade executive officer. The crossing area commander controls engineer regulating points, holding areas, MP checkpoints, and crossing sites. The brigade commander provides IEW support to the crossing area commander from those IEW assets allocated to the brigade, most notably GSR teams.

SUPPORT

MI units contribute to the planning and execution phases of river crossing operations. IPB enables the commander to select the best crossing site and know the battlefield beyond, so that operations can be sustained without interruption. IEW resources deploy forward and continue seeking enemy weaknesses for exploitation and to warn of enemy forces capable of affecting the operation. Other elements guard the flanks to prevent enemy surprise. By identifying, locating, and tracking enemy NBC-capable delivery systems, MI resources further help the commander know the battlefield and guard against a surprise counterattack.

MI units supporting an offensive that includes a river crossing operation seek to deny the enemy knowledge of the time and place of crossing. The force commander may direct that a deception plan be executed to further confuse the enemy. Such plans require positive C^2 at the highest tactical level to ensure success. MI units provide ICD, jamming, CI support, and the full range of intelligence support.

PLANNING AND EXECUTION

Crossing operations require detailed and thorough IPB planning at corps or higher, normally starting weeks and even months before a crossing is executed. The length of long-range IPB planning will depend on the severity of the obstacle and the intelligence assessment of a likely enemy capability to resist.

The division commander starts the staff planning process which leads to formulation of the commander's concept of the operation. Based on the picture of the battlefield drawn by the G2 as a result of IPB and the G3's assessment and estimate of resource supportability, the commander decides whether the crossing will be—

- ☐ Hasty or deliberate.
- ☐ Day or night.
- ☐ Wide or narrow on the front.

A crossing force commander is then selected. The division G2 and G3 normally designate one of their assistants to serve on the staff of the crossing force, or they serve on that staff themselves. The MI battalion commander or S3 serves as the crossing force commander's IEW executor.

The crossing force commander facilitates planning by dividing the operation into four distinct and manageable segments:

- ☐ Advance to the river.
- ☐ Assault crossing of the river.
- ☐ Advance from the exit bank.
- ☐ Securing the bridgehead.

The execution phase of the river crossing is accomplished by dividing the force into four separate groupings:

- ☐ Assault forces.
- ☐ Follow-up forces.
- ☐ Support forces.
- ☐ CSS forces.

Assault Forces

Assault forces make the initial assault on the river and continue until final objectives are secured. They cross the river by any means available and move as rapidly as possible. In order of priority they ford, swim, raft across, or bridge the river. MI units normally are not part of the assault force; however, GSR teams may accompany the assault force if exit bank surveillance of enemy approaches to the crossing site cannot be conducted from the entry bank. GSR may also guide assault forces through obscuration. Aerial ESM and surveillance systems directly support the assault force, add depth to the IEW support, and provide early warning of enemy counterattack and movement of the enemy reserve. They also provide ELINT support and cue ground-based ELINT systems.

The crossing force commander also considers using airborne and air assault forces to secure terrain objectives in the bridgehead area. Should such forces be used, the assault force is responsible to linkup with these forces. Man-packed ESM and GSR and interrogation teams may accompany airborne and air assault forces performing such missions. Such support enhances the IEW support available to the crossing force commander and helps sustain the momentum of the attack.

MI units must clarify the enemy situation on the exit bank before the operation is launched to ensure that the full value of artillery and offensive air support are brought against HVTs. In addition, maximum use of smoke is essential, as is full exploitation of ECM to "freeze" enemy units in place and deny them the ability to orchestrate a counterattack.

Follow-Up Forces

Follow-up forces move close behind the assault force and provide support as required. The majority of MI assets are part of this group. They provide support from the entry bank; read the battle on the exit bank to identify enemy disposition, strengths, and weaknesses; and provide ECM support against enemy fire direction and air defense communications nets. As consolidation progresses, MI units concentrate on developing the situation to continue the attack and provide flank security for the shoulders of the bridgehead. Enemy defenses on the exit bank are identified, located, and defeated. At the same time, interrogation, CI, and S&T intelligence teams carefully study and exploit sources for information which will enhance the continuation of the attack without loss of momentum.

Continuous support of close operations provides the time necessary to build combat power on the far side of the crossing and to continue the offensive. For a detailed discussion of the various control measures used in this phase, see FM 90-13.

Support Forces

Support forces provide engineering and traffic control support to the crossing force commander to ensure momentum through the crossing area.

Combat Service Support

Combat service support units sustain the attack. MI and other unit trains establish themselves in forward areas of the bridgehead to get ready for continuation of the attack. Rearming, refueling, and maintenance points are established along advance routes to speed servicing.

CHAPTER 8

Defensive Operations

Defensive operations can retain ground, deny the enemy access to an area, and damage or destroy attacking forces. They cannot, however, win the battle by imposing the will of the commander on the enemy. For this reason, the defense is a temporary expedient, undertaken only when it is impossible to conduct offensive operations, or when attacking in another area. All defensive actions are undertaken in anticipation of ultimately resuming the offense.

Corps and divisions fight unified defensive battles based on five elements:

- ☐ Continuous deep operations in the force's area of operations.
- ☐ Covering force operations to support the main effort.
- ☐ Close operations in the main battle area (MBA).
- ☐ Reserve operations either in the MBA or in the covering force area (CFA).
- ☐ Rear operations.

Deep operations, covering force operations, and operations in the MBA are planned and executed as complementary actions of a single unified battle plan supported by reserve and rear operations.

Commanders plan the overall defensive effort on the basis of the METT-T. MI assets are allocated within the elements of the organizational framework to support the overall scheme.

IEW PRINCIPLES

The IEW principles stated in Chapter 7 apply to the defense, as well as other operations. Slight variations in application may occur as priorities are changed to meet tactical requirements. The following paragraphs describe the particular application of IEW principles to the defense.

KNOWING THE BATTLEFIELD

In the defense, the commander has the best opportunity to know and control the battlefield in detail, and to maximize the exploitation of such knowledge. IEW elements, and MI units, in particular, are the key to seeing and controlling the battlefield. They perform IPB well before the defensive battle and provide detailed graphic analyses. These are reinforced by the personal reconnaissance of commanders and staffs. IPB not only helps the friendly commander to use terrain, but also to anticipate how the enemy will use it. Additionally, IPB identifies key terrain essential to the success of the defense.

Outnumbered and outgunned combat forces cannot be permitted to suffer surprise on the battlefield. IEW operations act in two ways to defeat enemy attempts to surprise the friendly commander. First, IEW provides intelligence and combat information which tells the commander what to expect from the attacker. Secondly, IEW supports OPSEC which denies the enemy information needed to set up situations which can surprise friendly forces. If enemy forces are unaware of the actual friendly defensive deployment, they will be unable to maneuver with certainty to attain surprise. IEW offers the commander one of the few capabilities to take the initiative away from the enemy by highlighting windows of opportunity for the conduct of offensive action.

MI units find, track, and target enemy forces for deep operations, enabling the commander to attack them most effectively at long range. They provide early warning of enemy approach in both the CFA and the MBA. They search for unexpected offensive opportunities. They also provide flank and rear security by finding, tracking, and targeting enveloping enemy units.

Collected information is analyzed to read enemy intentions and to provide early

warning. The enemy is capable of conducting a wide range of deception operations which pose a particularly serious threat. IEW elements must work to uncover enemy attempts at deception in time for the commander to react effectively.

The composite IEW support provided in the defense enables the commander to read the battlefield clearly. IEW tells the commander which enemy forces will attack and when, where, and how they intend to do it. This knowledge enables the commander to position weapons and forces to finish the assault force fight quickly and resume the offensive.

DENYING THE ENEMY INTELLIGENCE

Enemy uncertainty is key to defensive operations. Every opportunity to create uncertainty in the minds of the enemy commanders, to make them hesitate even slightly, or to make wrong decisions must be seized and developed. Enemy hesitation and wrong decisions permit the friendly commander to take the initiative.

IEW works toward this end by participating in and supporting deception operations, protecting friendly C^2 and emphasizing countersurveillance operations. Support to deception includes providing intelligence for planning and executing the operation. Participation includes the execution of IED actions, operating C-E equipment as part of MED and SED actions, and conducting operations which reinforce the deception objective. CI activities are oriented toward the protection of C^2, a critical function in the defense, especially since solid C^2 are essential to seizing the initiative.

DESTROYING AND DISRUPTING ENEMY C^3I

IEW elements contribute to the defense through ECM, CI, and S&T intelligence. Jamming is used to disrupt and degrade enemy C^2 at crucial times in the defensive battle. Enemy units are prevented from receiving orders essential to adjust their plan of attack. In essence, part of the battlefield is "frozen" long enough for the friendly commander to exploit a situation which otherwise would have been corrected by orders from the higher enemy command. Such efforts may prevent the enemy from concentrating, dispersing, maneuvering for envelopments, or exploiting momentary friendly vulnerabilities. Jamming is also used against enemy C^2 and air defense links to suppress fire support and air defense operations.

CI attacks the enemy's capability to collect intelligence concerning the friendly force. It contributes to OPSEC objectives of the friendly force and attacks enemy agents conducting espionage, sabotage, subversion, and terrorism.

S&T intelligence contributes to the defensive through the identification of technological weaknesses in enemy systems. Although these actions are applicable to all operations, countermeasures developed through S&T intelligence may be most effective in defense operations.

MAINTAINING INTEGRITY OF OPERATIONS

IEW units are organized in depth to provide flexibility and maintain the integrity of IEW operations in the defense. Resources are task organized to meet all requirements of a single, unified battle through the assignment of appropriate resources to close or deep operations. Generally, control is centralized with resources deployed throughout the battle area. In close operations, IEW support is weighted in favor of the most likely approach to defensive positions. In deep operations, support is weighted in favor of the most lucrative approach in terms of NAIs and HVTs. Other IEW resources must be used to cover gaps, flanks, unit boundaries, and other areas where combat power is weak, or where coordination is less than desired. Flexibility is essential in all task organization and deployment schemes for the defense. The IEW system must be capable of reacting to both friendly- and enemy-initiated changes in the tactical situation. The IEW system supports every aspect of the defensive battle. Units are deployed early to provide combat information, targeting data, and intelligence to support deep operations, covering force, and MBA.

DEEP OPERATIONS

Deep operations begin before the enemy closes with the friendly force. They go on throughout the CFA and MBA engagements, and will usually continue after direct contact between forces has ended.

In conducting deep operations, the commander focuses the intelligence collection effort on areas and units of particular concern, while maintaining a current intelligence picture of enemy forces throughout the area of interest. As enemy formations approach the FLOT, the commander monitors their movement, seeks HVTs, and initiates deep attack options.

Deep operations, designed to wear down, delay, disrupt, and, where possible, to destroy enemy second-echelon forces, require detailed planning and coordination. Limited strike and acquisition means must be efficiently employed, allowing no margin for waste or error. Deep operations, so essential to a sustained and effective defense, are highly dependent on responsive IEW support.

IEW support of deep operations consists of two primary tasks: Identifying the enemy's main effort, and target development. Each of these actions is critical to the successful interdiction of the enemy's second and follow-on echelons.

IDENTIFY MAIN EFFORT

The first task for IEW support, once the battle begins, is to identify the enemy's main effort as early as possible. Time is essential. The commander must have time to plan the operation, both deep and close; request release authority for nuclear and chemical weapons, if to be used; and prepare resources to execute the plan. IPB is the starting point and its products are used to direct collection activities and to cue analysis elements.

Collection resources first orient on finding and tracking enemy formations and then on updating the information as often as necessary. Analysis elements use collected data and IPB products to determine the enemy's composition, disposition, strength, rate of movement, and intentions. When necessary, they cue collection operations to produce data needed to answer specific questions. Analysts also maintain a constant watch for enemy attempts at deception.

TARGET DEVELOPMENT

Target development begins simultaneously with actions to determine the enemy's main effort. IPB assists in target selection, and the G2 provides advice on priorities and values assigned to probable targets. Collection operations are initiated to locate and assess HVTs such as bridges, defiles, and similar targets. As soon as the main effort is identified, targeted enemy forces are tracked to provide data on when they will arrive at the attack point. Analysts cue the G3 staff in time to permit attacking the target's point of highest value. Once the target has been attacked, collection and analysis resources are used to determine the effectiveness of the attack in terms of a damage assessment and if the objective of the attack was reached.

The intelligence assessment of targets before and after the attack is essential to the air-land battle. The commander must keep follow-on echelons away from the MBA until close operations are won. Only by knowledge of the effectiveness of deep operations will the commander be able to see the accomplishment of this part of the mission.

Just a few organic IEW resources are capable of supporting deep operations at corps and division levels. Aerial systems and long-range surveillance units are the primary organic resources available for seeing deep. Therefore, corps and division rely on EAC, other services, and national systems for much of the intelligence required.

Aerial resources of the corps and divisions are coordinated to provide 24-hour surveillance to the greatest depth possible. SLAR provides MTI coverage from which enemy movement patterns and target concentrations may be discerned. When absolutely essential, aerial photographic and infrared missions may cross the FLOT to acquire imagery of critical targets. Aerial

COMINT and ELINT systems collect information on enemy C^2 communications and noncommunications systems. Long-range patrols, when available, provide detailed HUMINT on activities and locations deemed critical to deep operations. The fusion of this information provides part of the intelligence needed to find, track, and target enemy second-echelon forces.

Other services, especially the USAF, provide additional data on the area covered by Army systems and extend the range over which surveillance is maintained. EAC and national systems complement this coverage and extend surveillance well beyond the FLOT.

The complete picture needed for deep operations can only come from the integrated use of collection resources available at tactical and strategic levels, and from the fusion of the resultant data. Time is a critical factor, especially in the targeting function. Planning must consider the time required to identify the target, its movement into the target area, and the initiation and execution of attack options.

Additional considerations for the employment of IEW resources in support of deep operations include—

- Centralizing control of deep operations assets.
- Ensuring that resource deployment permits agility.
- Synchronizing resource deployment with maneuver battle plans to ensure direct, positive contributions to winning the battle.

COVERING FORCE

The second aspect in the organization of the defensive battle is the covering force operation. The commander organizes a covering force and deploys it forward of the MBA to—

- Force the enemy to reveal the main attack.
- Deceive the enemy.
- Strip away enemy air defenses.
- Delay the enemy.

MI units deploy to support the covering force battle. Reconnaissance and surveillance actions extend the capabilities of the covering force to collect essential information. Jamming can provide electronic screening and disruption, which reinforces combat power. CI support helps to preserve the combat power of units fighting the battle.

IEW support to the covering force battle consists of four primary tasks:

- Providing early warning.
- Contributing ECM to the combat power of the force.
- Targeting.
- Supporting deception.

Each of these actions contributes directly to the success of the covering force mission.

The IEW system provides early warning by locating and tracking enemy units at extended ranges. Corps and division aerial assets, supported with intelligence from EAC and national agencies, provide the earliest warnings of the enemy's approach. As enemy units close on the CFA, shorter-ranged resources assume the tracking function. Targeting begins beyond the maximum range of weapons available to the covering force.

Identification of the enemy's main attack is an essential element of the covering force mission. IEW resources identify the enemy force most likely intended for the main attack. Other enemy forces are identified in terms of relative strength, composition, direction of movement, and probable mission. This data permits the covering force commander to concentrate on positions which oppose the probable main attack and any supporting attacks. Concentration is possible through economy of force actions which include the deployment of MI elements to monitor thinly-held or undefended avenues of approach. Simultaneously, MI resources are deployed to the flanks to provide continuous surveillance.

As the enemy force encounters the covering force resistance, reconnaissance and

advance guard elements attempt to overcome or bypass the friendly force. If the covering force's combat power has been concentrated at the right place and time, sufficient resistance will be applied to stop the advance elements and force deployment of the main body. As the main body deploys, IEW resources monitor the action to identify more clearly the enemy commander's intentions. It is also crucial at this point to provide detailed combat information and intelligence to the covering force commander about the progress of enemy deployment. At the critical time before decisive engagement, the covering force commander initiates a delaying action back to the MBA. Concentration of covering force combat power and the subsequent delaying actions may represent targets for enemy NBC weapons. Therefore, IEW resources closely monitor NBC delivery systems and provide early warning of their intended use.

The decentralized, fluid nature of the covering force battle requires interrogation support at the lowest possible echelon. This requires DS interrogation teams from the supporting MI companies, battalions, and corps MI brigade. Questioning of civilians and EPWs is brief, and is conducted to gain information of immediate tactical value. Interrogators gather information about the identification, composition, location or direction of movement, strength, and capabilities of enemy forces involved in the immediate covering force battle.

ESM resources support the covering force from successive positions established along each phase line. ESM assets are used against the following types of targets during the initial and subsequent covering force engagements:

- Reconnaissance nets.
- C^2 nets between first-echelon battalions, regiments, and divisions.
- C^2 nets associated with artillery and rocket units, especially those with an NBC capability.
- Communications and noncommunications jammers.
- Surveillance radars located with reconnaissance forces.
- Countermortar and counterbattery radars.
- Air defense radars.

Aerial ESM resources are used to overcome LOS and mobility limitations and fill gaps in coverage left by ground resources. Use of aerial resources is closely coordinated with ground resources. A major advantage in using aerial resources is that they are capable of cuing ground ESM resources and GSR.

GSR teams support the covering force by providing early warning of approaching enemy forces and the detection and location of lead elements for targeting at maximum range. The teams—

- Continuously search avenues of approach to detect or locate enemy activity.
- Monitor choke points, such as bridges or road junctions.
- Increase effectiveness of fire support by detecting and accurately locating targets.
- Provide surveillance of gaps between deployed units.

Corps aerial resources, especially SLAR, provide continuous updates on the movement of enemy forces toward the deployed covering force. This supports the interdiction effort of deep operations and keeps the covering force commander aware of the enemy force disposition.

A significant portion of the C^3CM available to the covering force is in the ECM systems deployed for its support. ECM systems initially jam C^2 communications among reconnaissance elements, the advance guard, and the main body. The intent is to disrupt reports to the enemy force commander and to prevent or disrupt orders sent to the advance elements. As the enemy main body begins to deploy, ECM assets jam C^2 communications to slow deployment and to inject as much confusion as possible. ECM also provide electronic screening for OPSEC.

Targeting is vital to the covering force operation. Since the strength of the covering force is limited, it is essential that available weapons concentrate on destroying HVTs. IEW resources seek out and assess the value of specific targets and make nominations to the operations staff. Both primary and alternate targets are then tracked so that they can be attacked at their time and place of peak value to the enemy commander. Destruction of HVTs contributes to the covering force mission by delaying the enemy main attack and weakening enemy combat power.

The principal deception conducted by the covering force is to make the enemy commander believe that the friendly main force has been encountered. IEW contributes to this deception by supporting OPSEC, conducting limited ICD, and participating in the command's tactical cover and deception operations.

CI teams are employed in GS and operate throughout the CFA. They monitor friendly OPSEC procedures and, in conjunction with the processing elements, provide information to the commander concerning enemy collection capabilities. They recommend OPSEC and deception measures.

The types of MI resources supporting the covering force are dependent on whether a division or corps exercises control of the covering force. A division covering force is normally supported by task organized elements of the divisional MI battalion. The corps covering force may include an ACR or divisional armored cavalry squadrons, brigades, or battalion task forces. When an ACR is involved, its organic MI company moves with, and supports, the ACR. Resources from the corps MI brigade may also be deployed forward. When divisional resources are a part of the corps covering force, each division provides the appropriate MI elements to support them.

Command and control of MI units is established at the discretion of the covering force commander. Generally, the senior MI commander assigned to the covering force is given OPCON of all MI resources deployed forward. Generally, all elements located in the covering force element are attached to the covering force.

A prime consideration in selecting resources to support the covering force is mobility. The covering force mission requires a high degree of mobility, and MI units must have the same degree of mobility. Resources which are unable to keep up with the supported units or require excessive displacement time should not be deployed in the CFA.

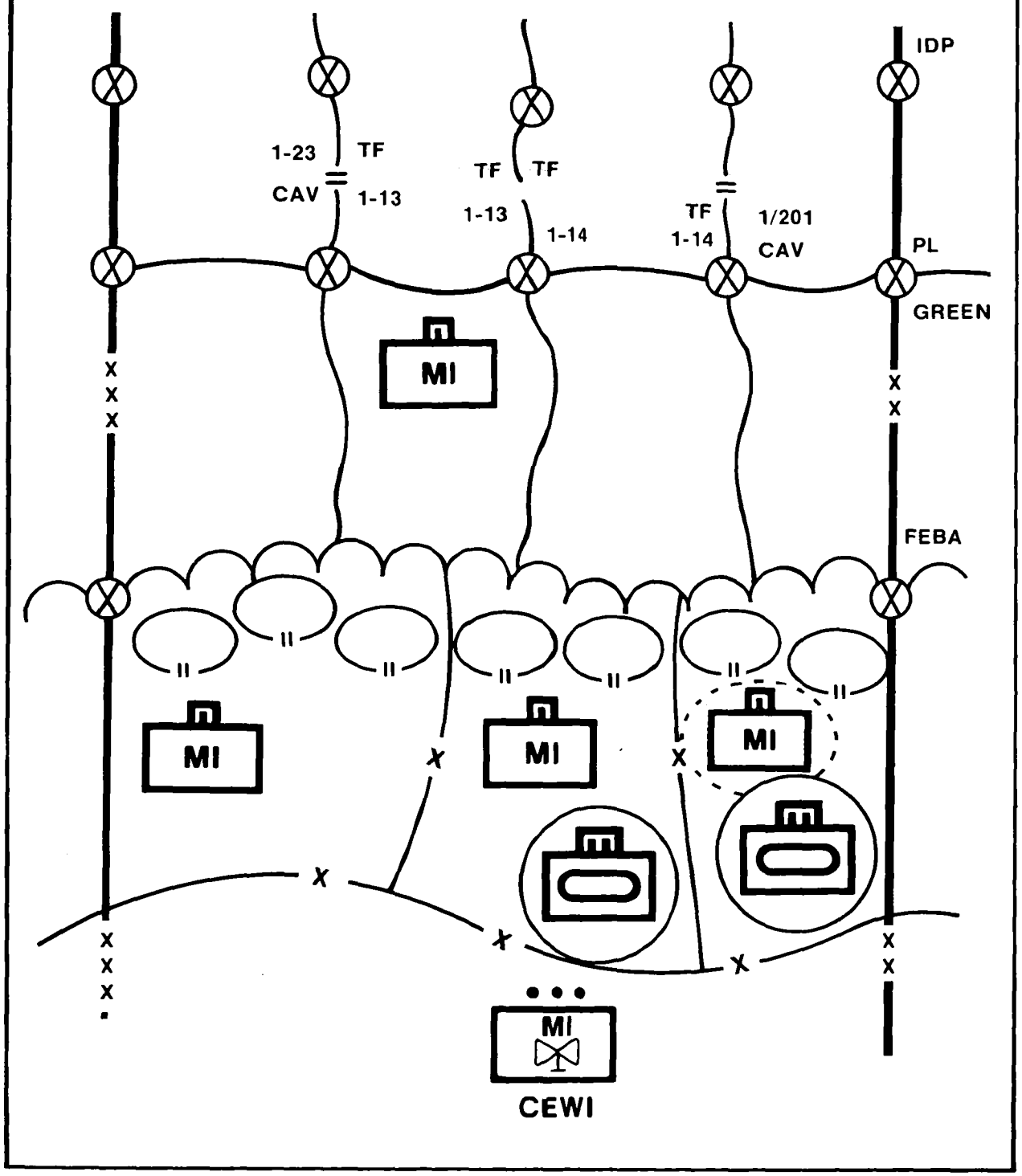
Resources supporting the covering force are deployed well forward in the CFA. Deployment positions are selected to provide the maximum forward coverage and appropriate security to enhance resource survivability. An additional deployment consideration is flexibility. MI resources must be positioned to respond quickly to changes in the tactical situation.

In line with flexibility is the exercise of decentralized control. Control is decentralized due to the normally extended front of the covering force and to the need for immediate reaction to changes in the tactical situation. Such flexibility is attained by delegating control to the lowest level capable of meeting mission requirements. Decentralized control increases the responsiveness of MI resources since each resource is allocated against those targets of greatest value to the local commander.

Concentration of MI resources is dependent on the desired effect. ECM resources normally are concentrated against high threat areas. Collection resources may first be concentrated against high threat areas and then dispersed to provide wide-area coverage to cover gaps and exposed flanks. Contingencies for ECM and collection resources are carefully planned to meet the flexibility required by the tactical situation.

The following illustration shows MI deployment for a division defense (covering force) operation.

MI DEPLOYMENT FOR A DIVISION DEFENSE (COVERING FORCE)



SUPPORT TO THE MAIN BATTLE

Success in close operations is dependent on knowing the enemy, terrain, and weather and deploying to heighten the natural advantages of the defense. IEW resources concentrate on tracking enemy forces, targeting, integrating ECM with fire and maneuver, and contributing to the security of the defending force.

Close operations, fought at close range in the MBA, rely more heavily on combat information than on intelligence. Immediate reports of enemy activities, weaknesses, and vulnerabilities are passed to commander, operations staff, and fire support system. Combat information provides the basis for friendly fire and maneuver to exploit exposed HVTs and to attack and destroy vulnerable enemy units. Local counterattacks, based on the overall intelligence picture of the battlefield, may be triggered by combat information.

Intelligence is used for the development of the battle plan, identification of enemy intentions, and the location and targeting of NBC-capable weapon systems. It also provides other data available only through analysis of multisource information.

IEW support is planned and executed to meet the priorities and established needs of the commander. Resources are task organized and deployed to support these priorities and to maintain flexibility to meet changing requirements. The priority of IEW efforts is generally in the area of the expected enemy main attack or other critical areas. Such efforts must be synchronized with the actions of other elements of the combined arms team to achieve maximum effect.

ECM are integrated with fire and maneuver to ensure that the actions of each are complementary and mutually supporting. ECM, in conjunction with fire support, attack enemy C^2 communications to disrupt, delay, and disorganize enemy forces before, during, and after entry into close operations.

The defense, especially in close operations, depends on effective OPSEC. Friendly strengths, weaknesses, and intentions must be hidden or falsely represented to the enemy. The enemy must be lured into action favorable to the friendly commander. IEW supports these actions by determining enemy collection capabilities and by developing countermeasures to be applied by the friendly force. IEW monitors the OPSEC posture of the friendly force to determine how much the enemy can collect about friendly disposition, composition, strength, and intentions.

IEW supports deception through IED and by providing the intelligence necessary to plan and conduct the operation. Accurate assessments of enemy vulnerability to deception, and the effectiveness of the deception, are critical to the success of the defense.

IEW resources are used to provide early warning of threats against exposed flanks or gaps in defensive positions. Especially important is the detection and early warning of enemy attempts to envelop the defending force.

As the covering force withdraws into the main defensive positions, IEW assets are redeployed to support close operations. Resources organic to the ACR remain with the regiment to support the planned use of the ACR. Division and corps assets revert to division or corps control. Generally, corps resources which normally support divisions are placed under the control of the divisional MI battalions. Other resources normally under corps control are assigned new missions by the MI brigade.

Close operations are conducted by brigades, and are orchestrated and supported by the division. Short-range IEW resources are deployed well forward to support brigade close operations. Generally, the brigade or division blocking the avenue of approach of the main attack is weighted more heavily with IEW assets. Other sectors are provided support essential to defeat supporting attacks and to cover gaps or weaknesses. When necessary, MI resources are deployed to maintain surveillance over assailable flanks. The deployment of

resources is in accordance with the commander's battle plan for both the defense and the assumption of the offense. Generally, MI support to brigade operations requires a high degree of centralized control and decentralized execution.

Interrogation teams generally deploy forward to immediately exploit EPWs for combat information usable by the brigade commanders. Teams, when supported with additional interrogators from corps, deploy to brigade and division EPW collecting points established by the MPs. At each of these collecting points, EPWs are subjected to rapid interrogations designed to obtain information of immediate value. Further interrogation may be conducted at the division central EPW collecting point, in the corps EPW holding area, or in the communications zone EPW camps.

Ground-based ESM resources, supported by aerial missions, concentrate on enemy first-echelon forces. ESM systems target C^2, fire support, air defense, and other critical elements of the enemy force. Destruction of these elements, or temporary disruption through ECM, weakens the attacker quickly, creates confusion, and builds opportunities for enemy mistakes. These mistakes lead to exploitable vulnerabilities. Generally, ESM systems in close operations concentrate on—

- Enemy REC elements, especially communications jammers.
- C^2 nets between battalions and regiments.
- Regiment and division fire support systems.
- Surveillance radars with first-echelon battalions.
- Air defense radars with first-echelon regiments.
- Countermortar and counterbattery radars.
- Meteorological radars.

GSR teams may be deployed to target enemy assault forces, to overcome obscuration caused by weather or battlefield smoke, or to cover gaps and exposed flanks. When used to target the assault force, GSR teams provide highly accurate data to indirect fire systems for immediate attack of the target. When deployed in gaps or on flanks, the GSR teams increase the combat power of defending elements by providing early warning of enemy activity and by targeting the enemy force at maximum range.

Aerial resources may provide limited support to close operations; however, they usually are concentrated against follow-on enemy forces in the deep operations area. The simultaneous execution of coordinated deep and close operations is crucial to the success of the air-land battle. Therefore, the dividing line on MI system deployment is generally one of range. Long-range assets concentrate on deep operations while close operations support is provided by shorter-range resources.

ECM are as important to close operations as they are to the covering force operations. Aerial and ground ECM systems are concentrated against the main attack to maximize the combat power of the defender. Concentration for ECM is not necessarily physical. Depending on range, LOS, and power requirements, jammers are deployed for flexibility and survivability. They must also be ready to switch from the main attack to a supporting attack, should the supporting attack appear to be succeeding.

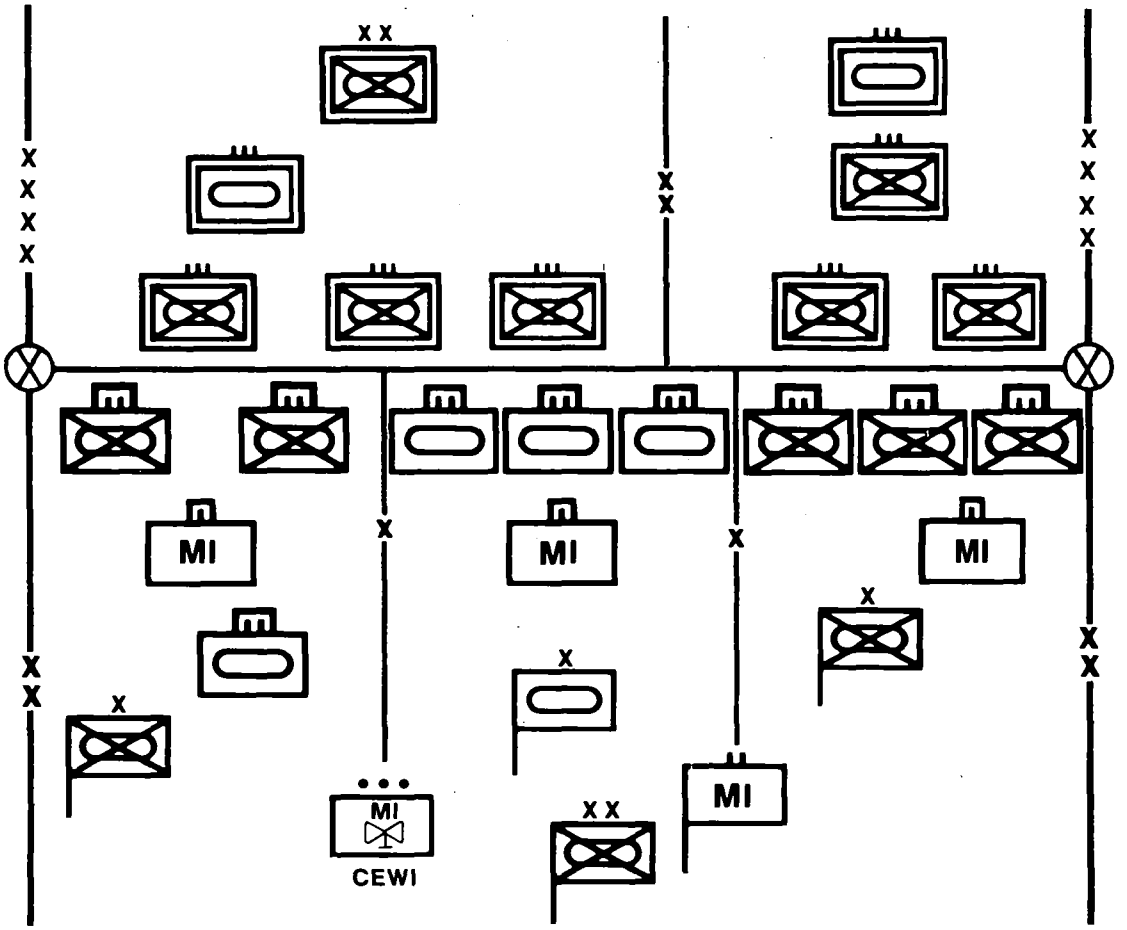
OPSEC in close operations, as stated previously, is essential to maximize the natural advantages of the defense. OPSEC evaluation teams deploy before and during the battle to support brigade OPSEC requirements. It is essential that OPSEC and IEW support to deception help conceal friendly strengths, weaknesses, and intentions.

The following illustration shows a type of MI deployment for support to division close operations.

Defensive operations stated in this chapter are based on the premise that the commander will seize the initiative at every opportunity and proceed with an offensive operation. Under certain conditions, the commander may choose to withdraw from

the CFA or MBA. This type of operation is covered in Chapter 9.

MI DEPLOYMENT FOR DIVISION DEFENSE (CLOSE OPERATIONS)



CHAPTER 9
Retrograde Operations

Retrograde operations are organized movements away from the enemy that relinquish terrain to enemy control. Such operations may be forced by enemy action or executed voluntarily. Unlike the defense, the intent of retrograde operations is to avoid decisive engagement.

The primary purpose of retrograde operations is to preserve the integrity of the force, so that, at some future point, the offense may be resumed under more favorable conditions. Retrograde operations are also conducted to—

- Harass, exhaust, resist, delay, and inflict damage on the enemy.
- Draw the enemy into an unfavorable position.
- Permit the use of forces elsewhere.
- Avoid combat under unfavorable conditions.
- Gain time.
- Reposition forces.
- Shorten lines of communications.

There are three types of retrograde operations: delay, withdrawal, and retirement.

In the delay, units trade space for time without losing freedom of maneuver, while inflicting the greatest possible punishment on the enemy.

During withdrawal, units disengage from the enemy voluntarily to gain freedom for a new mission. Withdrawals are conducted with or without enemy pressure and may be assisted by another unit.

In a retirement operation, units not in contact with the enemy conduct an administrative movement to the rear. Retirement operations are not described in this chapter.

IEW PRINCIPLES

Retrograde operations increase the demands on the IEW systems by combining all aspects of offensive and defensive operations. When conducting retrograde operations, commanders require highly accurate, timely information in order to make decisions and execute, at the precise time, specific actions associated with each combat operation.

Commanders require the clearest possible picture of the enemy's disposition and the terrain over which the operation is to be conducted. The focus of intelligence operations is on—

- Locating and tracking enemy forces.
- Determining when and where the enemy will attempt to mass combat power to overtake and destroy the friendly force.
- Identifying natural obstacles and related key terrain around which the commander plans and conducts a delay or withdrawal operation. Priority of effort is given to detecting enemy attempts to outflank and isolate friendly forces. IPB identifies routes to enhance force security and mask friendly activities from enemy observation.

IEW support to C^3CM is oriented on destroying or disrupting key enemy C^2 and intelligence links during critical periods of the operation. Especially critical is the period when enemy forces have been stopped and forced to deploy. When this occurs, the delaying force must break contact and withdraw to avoid becoming decisively engaged. Destruction or disruption of key enemy links during this period delays enemy response to the disengagement and withdrawal. This gains the friendly force additional time to prepare and occupy the next delay position. Electronic deception is also used to deceive the enemy as to when disengagement has occurred.

OPSEC and deception are essential to the successful conduct of retrograde operations.

CI supports OPSEC by assisting the G3 to identify those critical friendly activities that must be protected to keep the enemy uncertain of the time and place of actual disengagement. IEW systems are used both physically and electronically to deceive the enemy about the disposition of the friendly force. IEW support concentrates on those measures that obscure the size and intent of the delaying force and preserve the element of surprise. Each time enemy commanders are engaged by the delaying force, they must be convinced through the application of combat power, OPSEC, and deception that they have engaged the main force. This causes them to deploy their forces, reinforce, and prepare to sustain an attack. The delay incurred is the purpose of the delay operation. In addition, the operation creates a situation in which the enemy commander may expose weaknesses and vulnerabilities that the friendly force can exploit to regain the initiative.

In retrograde operations, centralized control of IEW resources is required. This enables the IEW coordinators to draw upon the full spectrum of division, corps, and EAC assets to achieve the support required for the operation. GSR and ESM assets are located well forward to ensure maximum coverage of flanks, gaps, and thinly held areas. The organization of IEW support must be flexible enough to provide DS to brigades as required, give support to the force as a whole, and be capable of transitioning immediately to support follow-on operations.

DELAYING

Units assigned a delay mission will conduct a series of operations which are designed to retain the initiative while trading as little space for as much time as possible. These operations consist of varying combinations of attack, defense, screen, ambush, raid, and feint. They are conducted within a framework of two basic types of operational techniques—delay from successive positions and delay from alternate positions. A combination of both also may be used. The selection of technique is based on the factors of METT-T.

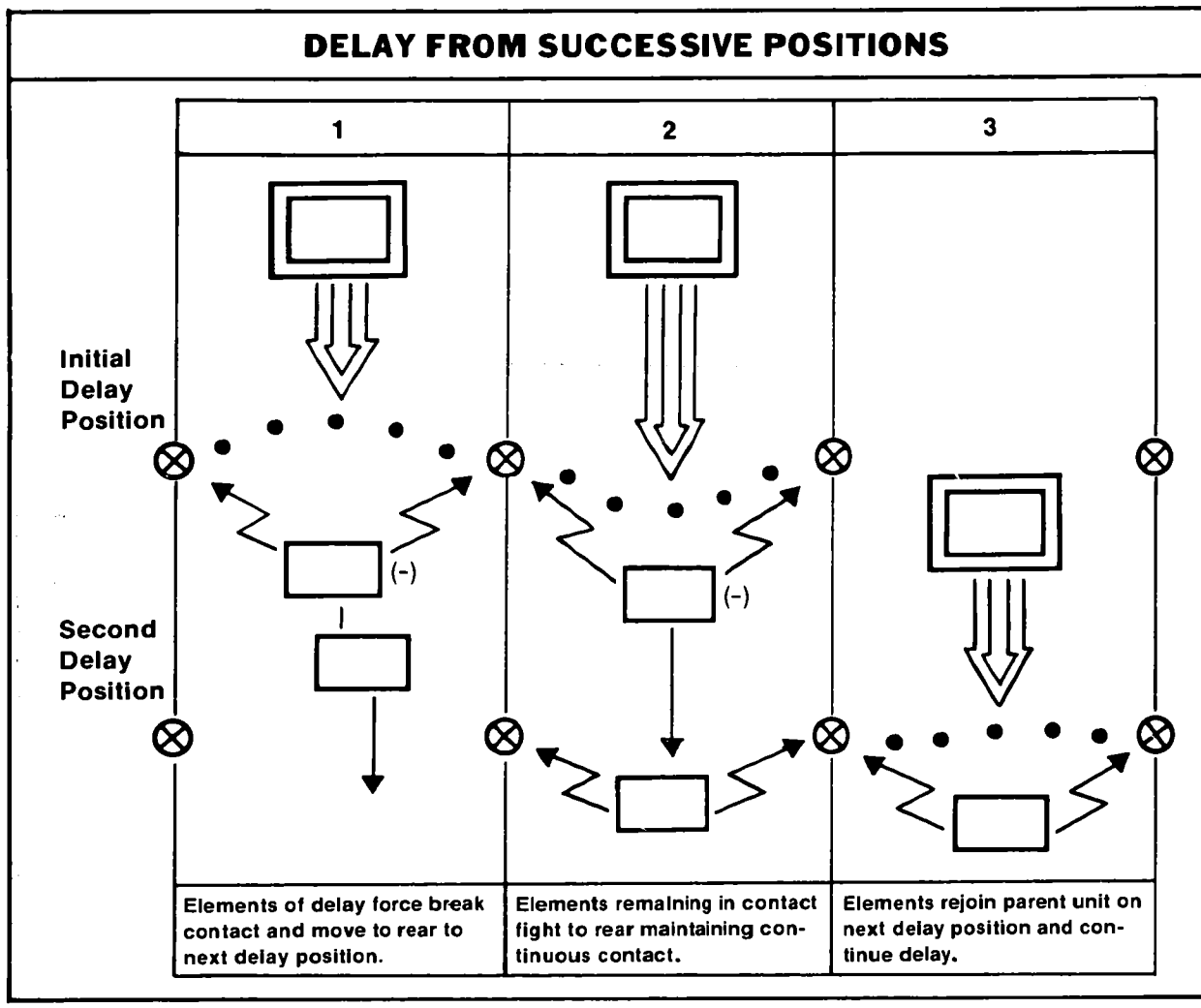
DELAY FROM SUCCESSIVE POSITIONS

This technique is used when the sector is so wide that available forces cannot occupy more than a single tier of positions simultaneously. It requires units to continuously delay at or between positions and is characterized by simplicity of control, minimum preparation of positions, and less depth of forces. It is more easily penetrated than the delay from alternate positions technique. A graphic representation of the delay from successive positions technique is shown in the following illustration.

Delay from successive positions is most frequently conducted at division and brigade levels. This tactic requires that the majority of available forces deploy forward along the most critical sector. Due to the inherent vulnerability to flank penetration, the forces provide major mission support to units conducting an economy of force screen along the flanks. This frees the maximum number of maneuver units for the major avenue of approach, since selection of this tactic presumes a thinly spread force over a wide front.

IPB efforts identify a series of delay positions which maximize the natural value of terrain. As time permits, these positions are improved and occupied before or after contact with the enemy is established.

Ground surveillance radar and CI elements (when available) of the MI battalion will directly support brigade commanders in maintaining contact with the enemy, help them identify local counterattack opportunities, and ensure security. The remaining MI battalion elements will operate in a GS, general support reinforcing, or reinforcing role to allow flexibility. The bulk of these forces is located in positions behind the initial delay position (IDP) and focuses on developing the situation in the deep operations area. CI personnel enhance the force OPSEC posture by advising units on concealment of locations, secondary delay positions (SDP), and times and routes of withdrawal. Areas behind the IDP are cleared of information which would be of



use to enemy intelligence. Target development is emphasized after situation determination is completed. As the enemy moves closer to IDPs, TAIs selected in the IPB process are attacked and ECM are integrated with fire and maneuver as the enemy repeatedly concentrates on the various TAIs. This process continues until decisive engagement is likely.

Withdrawal from the IDP begins on the order of the next higher commander. MI resources behind the IDP reinforce forward deployed MI units and assume their coverage to permit their displacement to the SDP. MI units along the flanks between the IDP and SDP maintain their positions until physically relieved and picked up by withdrawing IDP forces. Upon completion of SDP occupation by IDP forces, MI units originally on the SDP begin a phased withdrawal back to the next delay position. This process is completed for each successive delay position. During this displacement, aerial platforms provide the majority of deep operations coverage.

ECM missions are carefully controlled. Centralized control is maintained while providing close support to brigade commanders. Control is exercised by the MI battalion, based on the tactical situation and G3 guidance.

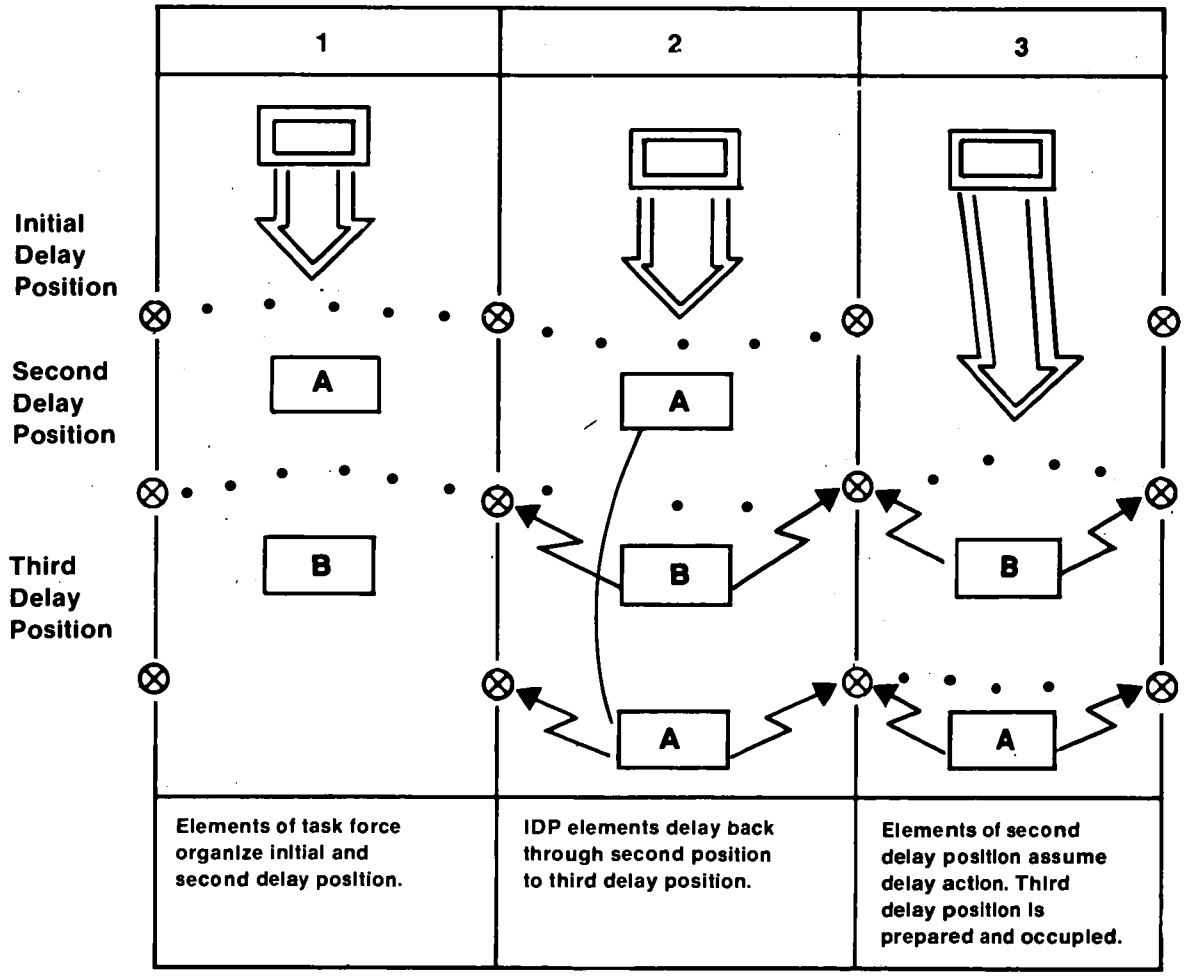
DELAY FROM ALTERNATE POSITIONS

The principal difference between alternate and successive delay operations is that, in the alternate system, two units are

used in a single sector. Each delays alternately. While the first is fighting, the second occupies the next delay position in depth and prepares to assume delay responsibility. As the first disengages and passes through or around the second unit, the second unit takes up the fight. The first unit then occupies a deeper position and prepares to subsequently resume the delay. Delay from alternate positions is characterized by continuous, more complicated coordination of fire and maneuver; requires more forces; and provides greater security. It is also more difficult to maintain contact with the enemy. A graphic representation of this technique is shown in the following illustration.

The delay from alternate positions is characterized by a higher density of forces operating on a narrow front. In these operations the IEW company team may be given a DS role due to the greater combat information requirements generated by unexpected enemy initiatives. The remaining MI resources are given a GS, general support reinforcing, or reinforcing mission. However, due to the complicated nature of this operation, a larger portion of resources is given either general support reinforcing or reinforcing on order missions in support of forward deployed units.

DELAY FROM ALTERNATE POSITIONS



WITHDRAWAL

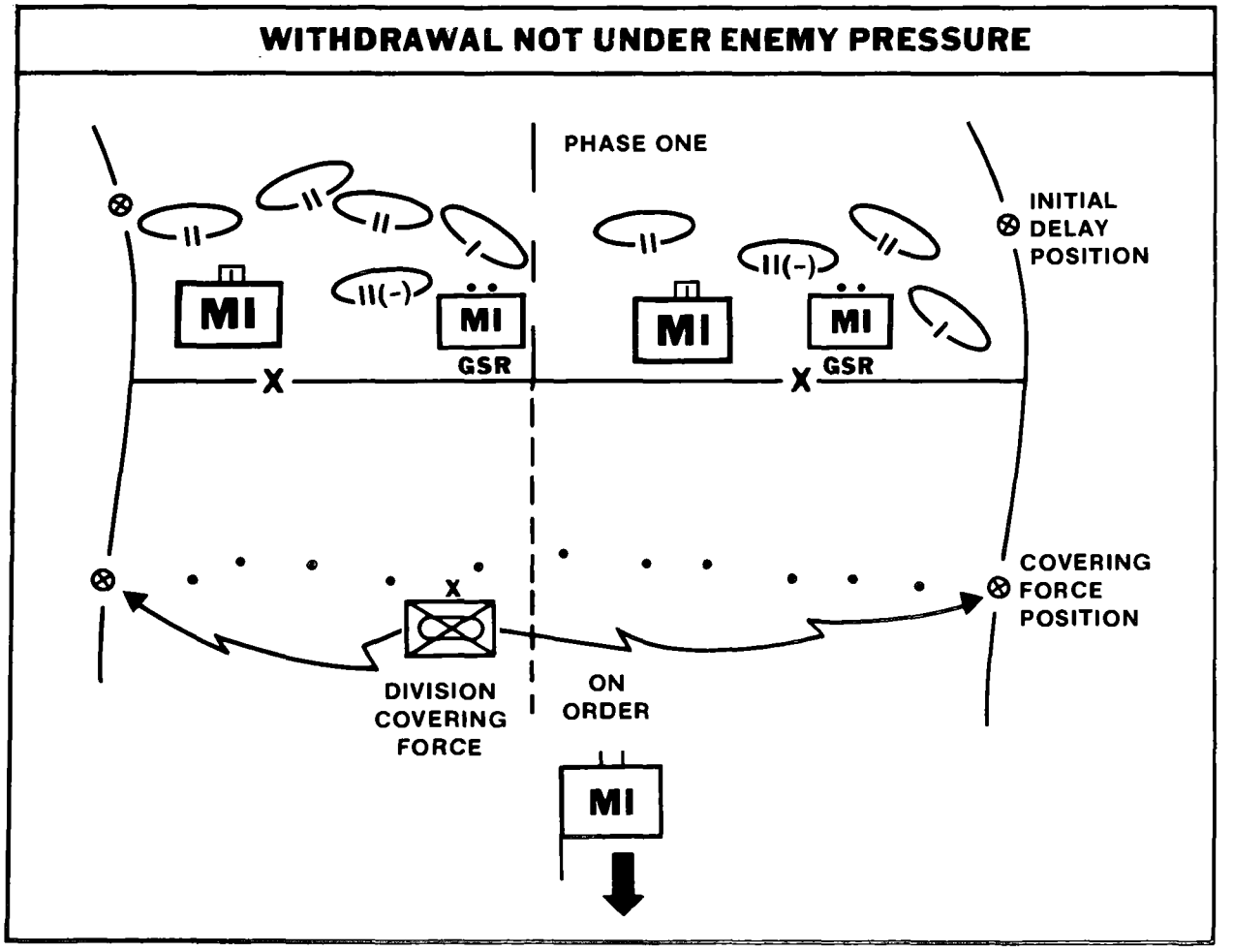
Units assigned a withdrawal mission maintain contact with the enemy to provide security and deception and to prevent a rapid enemy advance. Withdrawals, like delays, are facilitated by the conduct of—

- ☐ Limited objective attacks.
- ☐ Feints and ruses.
- ☐ Maximum use of limited visibility and darkness.
- ☐ Deep operation interdiction by conventional, chemical, and nuclear fires.
- ☐ Offensive air support.

Withdrawals are of two basic types—a withdrawal not under enemy pressure, and a withdrawal under enemy pressure.

A withdrawal not under enemy pressure is used by commanders to enhance freedom of maneuver and to minimize casualties. This type of withdrawal is characterized by centralized control and contingency planning to include alternate routes, priorities of movement, and effective traffic control. Other contingency actions may be necessary and should be planned. A graphic representation of this technique by operational phases is shown in the following illustration.

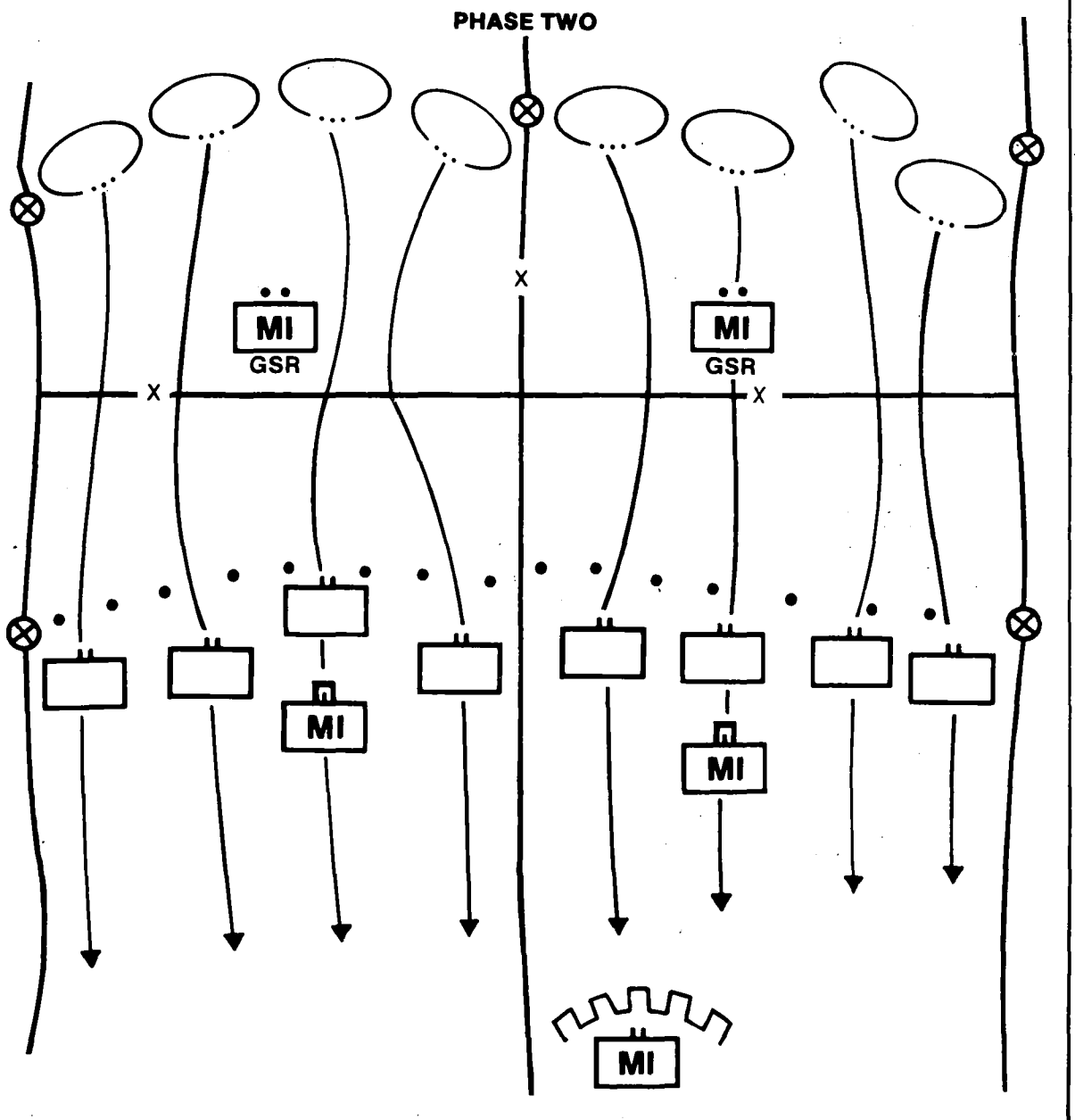
The withdrawal not under enemy pressure is begun by brigades and other units in contact by designating detachments left in contact (DLIC) to protect the first movement of the main body to the rear. DLIC also simulate a continuation of normal activity, representative of the larger unit, to mask the movement from enemy intelli-



gence. IEW resources, especially CI teams, play an important part in this action.

The simulation of normal unit activity is closely monitored by OPSEC evaluation teams based on the unit's signatures, patterns, and profiles. In addition to other OPSEC measures, fire and maneuver are employed to reduce the effectiveness of enemy collection capabilities. CI personnel assist MPs and civil affairs units in maintaining control of the civilian populace in the zone.

WITHDRAWAL NOT UNDER ENEMY PRESSURE



Based on previous IPB, intermediate delay positions and the final new positions will have been identified and the preparation begun. The division covering force, with appropriate MI support, is in place and ready to support the operation. The first elements to withdraw include combat support and CSS units not essential to support the DLIC. These elements normally include MI resources assigned reinforcing or general support reinforcing missions. Withdrawal of these units is followed by that of the main body, which includes nonessential MI assets. Finally, the DLIC and residual MI assets withdraw through the covering force into new positions. Both GSR and SLAR assets can help vector this force during periods of limited visibility and darkness. This sequence is shown in the illustration on the preceding page.

A withdrawal under enemy pressure differs significantly from the withdrawal without pressure. In this type of operation, units use delaying tactics to fight their way to the rear. All units initiate action simultaneously in a given sector. A covering force is highly desirable to assist the disengagement of committed units. It may also be used to initiate a counterattack. Key to the successful conduct of a withdrawal under enemy pressure is superior mobility, effective covering force employment, sound C^2, and local air superiority. A graphic representation of this technique is shown on the following page. IEW support and actions are similar to a delay from alternate positions.

RIVER CROSSINGS

River crossing operations conducted as part of delay or withdrawal operations are characterized by highly centralized control and detailed planning for IEW resources. They are conducted similarly to other phases of the retrograde; however, there are specific considerations applicable.

In conducting a crossing of a water obstacle in the delay, units not assigned missions and thus free to move execute a preplanned retirement across obstacles as quickly as possible.

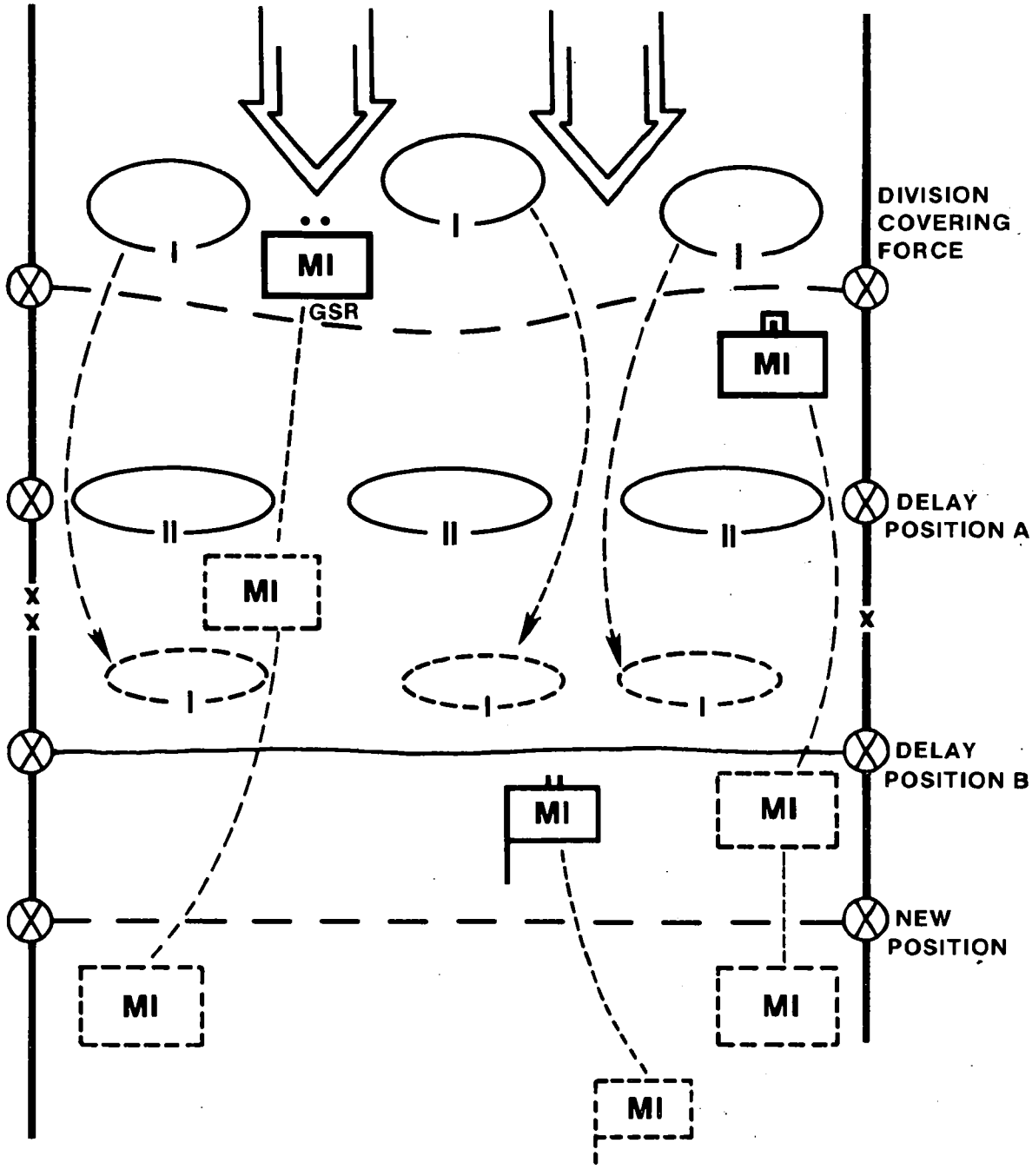
Those units scheduled to withdraw first are either given missions in the crossing area or assigned to overwatch defenses on the exit bank. MI units will usually not be withdrawn early because of their critical role in supporting the entire retrograde operation. The MI battalion tactical operations center and trains, however, retire early and, by close coordination with the corps MI brigade, maintain a continuous watch on the deep operations. Especially critical is airborne HF and multichannel intercept of enemy second-echelon communications by corps assets.

The delay will normally be continued until the battle is within communications and fire support range of the exit bank defense. At this point, forward of the holding line, the exit bank defense assumes responsibility for the battle.

The defense force is initially small. It develops plans for rapid lateral movement to cover likely contingencies. After the defense force has assumed responsibility for the battle, the requirement for close and continuous coordination becomes critical. Time and space constraints may have to be imposed to enable the entire delay force to cross the obstacle. MI units provide greater concentration on the flanks and other likely problem areas. Such economy of force missions enable more of the delay force to withdraw and establish a viable exit bank defense. CI teams sweep CPs, unit areas, and withdrawal routes to minimize anything of intelligence value falling into enemy hands. Selective use of ECM complements and supports mission success. ESM and surveillance aircraft are used to provide continuous coverage and to permit ground-based systems to cross the obstacle. If a counterattack is planned, stay-behind MI elements begin their preparation.

Activities in the crossing area do not differ significantly from the offensive crossing. The main difference is that friendly units have control over both entry and exit banks of the river. The actual turnover of responsibility from the crossing area commander to the defending commander is by mutual agreement or as directed.

WITHDRAWAL UNDER ENEMY PRESSURE



CHAPTER 10

Defense and Breakout of Encircled Forces

The nonlinear nature of the battlefield presents a high probability that units will find themselves encircled by enemy forces. This is especially true for maneuver brigades and battalions and the MI elements located within these forces. Encirclement may happen unexpectedly, due to a rapidly changing situation, or it may be by design.

A unit is considered to be encircled when all ground routes of evacuation and reinforcement are cut off by the enemy. The criteria for being encircled will differ, depending on unit mobility. For example, the circumstances of encirclement for a mechanized unit would differ from those of a light infantry unit. In either case, encirclement would most often happen when a unit is bypassed or cut off as a result of an enemy counterattack. Encirclement does not necessarily mean that a unit is surrounded by enemy forces in depth. An enemy force may occupy only scattered positions in the unit area and may not realize that the unit is located there, or know its size or composition. The unit must, unless ordered to hold its position, rapidly seize the initiative, exploit the advantages of enemy confusion, and break out before the enemy realizes what has happened. It is imperative that the encircled force commander have a clear understanding of the next higher commander's plan. Any action taken by the encircled force must coincide with, and reinforce, these plans.

DEFENSE

When a unit participates in a mission where encirclement is by design, or where the risk of encirclement is very high, the staff plans to—

- Continue the mission as long as possible.
- Establish an all-around defense and prepare for attacks by fire and maneuver, to include nuclear and chemical munitions.
- Break out or link up with relieving forces.

When encirclement is unforeseen, other actions must be rapidly accomplished. First, a defense must be organized and unity of command established. The senior commander in the encircled area normally controls all units therein. The immediate problem for the commander is the preservation of the force. The commander first evaluates the adequacy of the unit's all-around defense posture. Breakout is the next primary concern. The desires of the next higher commander concerning immediate breakout or defense of position must be determined. If the unit is to break out, an attempt should be made before the enemy forces can consolidate their position or take full advantage of the situation. If the encircled commander cannot break out, the defense is continued, a linkup is planned, and assistance is provided to the relieving force. Finally, a rapid reorganization and consolidation must occur. These actions also apply to MI units operating apart from supported maneuver units.

IEW support to an encircled force is crucial. The commander must have immediate intelligence concerning—

- The composition and disposition of encircling enemy forces and enemy forces capable of reinforcing.
- The exploitable weaknesses in enemy dispositions through which breakout and linkup can be effected.
- The enemy's intent to use nuclear and chemical weapons.

Additionally, the commander must have CI support to establish effective OPSEC. If a deception operation is part of the commander's plan, intelligence and CI support are critical. Finally, EW support, most

especially jamming, will be critical during breakout operations.

When MI units or elements are part of the encircled force, direct contributions are made to the commander's mission. Support provided by MI elements with the encircled force is carefully coordinated with the efforts of MI units with the main force. When no MI elements are in the encircled force, all support must be provided by the main force MI units.

IEW SUPPORT TO DEFENDING ENCIRCLED FORCE

ENCIRCLED FORCE COMMANDER	IEW SUPPORT
Re-establish chain of command.	• MI chain of command established. • Re-establish communications with higher (parent) MI unit.
Establish a viable defense.	• Orient on the dangerous avenue of approach. • Disperse and protect IEW systems for survivability. • Integrate MI elements into defensive plan.
Establish a reserve.	• Assign MI elements on-order missions to support commitment of reserves to contain penetrations/maintenance of interior lines.
Reorganize fire support.	• Establish procedures for integration of EW.
Reorganize force logistics.	• Centralize common supplies. • Enforce supply discipline. • Acquire external SIGINT/EW/GSR unique resupply if required, possibly by air drop or helicopter lift.
Establish security.	• Integrate IEW assets. • Provide CI support.

MI units or elements within the encircled force are generally placed under the temporary command of the senior MI officer (other than the G2 or S2). That officer is responsible for quickly reorganizing the MI elements available to support the mission of the encircled force commander. For example, if elements of two IEW company teams are with the encircled force, the senior company team commander takes charge of these MI elements. He may consolidate transcription and analysis teams from two C&J platoons to perform technical tasking of SIGINT/EW assets, until contact is regained with the division's TCAE. The reorganized units then respond to the commander and staff as the divisional MI battalion commander responds under normal circumstances.

The encircled force commander accomplishes those tasks listed in the left column of the chart on page 10-1. The G2 or S2 and MI commander support these tasks by initiating corresponding actions shown in the right column.

BREAKOUT

The attack to break out of an encirclement is conducted on a narrow front while a simultaneous defense is maintained in other sectors of the perimeter. To achieve a breakout, the encircled force commander accomplishes those tasks listed in the left column of the following chart. IEW supports the preparation for breakout by initiating those supportive actions in the right column.

An encircled force and its supporting MI unit are organized into four elements for the execution of breakout operations.

A rupture force opens a gap for the remainder of the encircled force to pass through. It holds the shoulders until the main body passes, then joins the rear guard. This force is usually armor-heavy and should be supported by GSR to see ahead of the rupture and to guide forces during limited visibility or darkness. Interrogators are used to screen prisoners and documents along the breakout corridor, and jammers disrupt the enemy communications to delay his decision cycle.

A reserve force assists the rupture force or assumes its mission. It then passes through the rupture force, maintaining the momentum of the breakout. The reserve force will normally pick up GSR, interrogation, and EW assets from the rupture force.

The main body consists of the encircled force commander's headquarters and most combat support and CSS elements. It moves as a single group following the reserve force through the rupture. Most remaining MI assets move with the main body, especially ESM systems which must provide support for the reserve force, the flanks, and the rear guard.

A rear guard deceives the enemy as to the location of the main effort and protects the rear of the force as it moves through the rupture. The rear guard, like a covering force, must contain representative elements to simulate the activities of the entire force. Under command of the force executive officer, the rear guard will normally contain such IEW assets as GSRs; a CI team to minimize information falling into enemy hands, especially from disabled equipment, supplies, and CPs; and ECM assets to disrupt the coherence of enemy actions and slow reinforcing units.

A graphic portrayal of the breakout force is shown on page 10-4. It highlights the distribution and allocation of MI assets normally supporting a brigade.

The rupture force moves over covered and concealed routes to attack positions. The rear guard stays in position to cover movement and to deceive the enemy.

Once the attack has started, momentum must be maintained. As the rear guard clears the penetration, the force moves on column axis toward the nearest friendly unit. If the distance is great, the force will move in a movement to contact formation for speed and increased security. Enemy forces along the route should be bypassed and reported. If bypass is not possible, a hasty attack is conducted from the movement to contact.

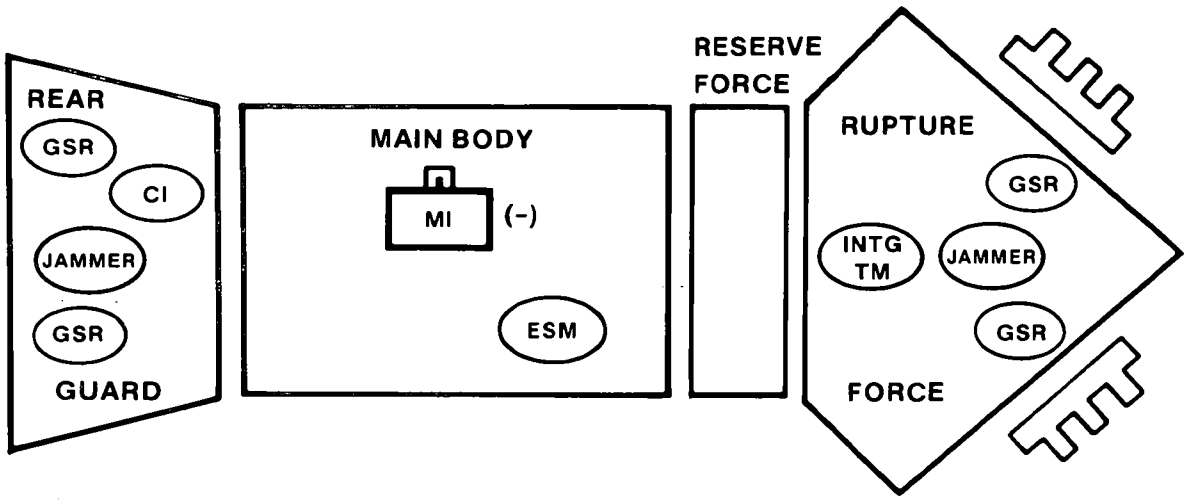
If a breakout is not possible, the encircled force may be relieved by another force attacking to defeat the encircling force. The encircled force commander must perform

the tasks in the left column of the chart on page 10-5 to effect a linkup. IEW supports these tasks through the actions in the right column.

IEW SUPPORT TO PREPARATIONS FOR BREAKOUT

ENCIRCLED FORCE COMMANDER	IEW SUPPORT	
Deceivas the enamy es to tha time and pleca of breekout	● Advises and essists in praparation of plen to include OPSEC aspects	● Provides CI and ECM support
Exploits gaps and weaknessas in anemy forces	● Idantifies enemy dispositions and possibla reinforcements ● Identifies axploitable edventages of weather and terrain, especially concealad routes ● Directs collection to fulfill information gaps	● Idantifies assailable weaknessas
Exploits darkness and limited visibility	● Uses GSR to guide forcas	● Uses GSR for targeting
Drganizas the breakout force	● Integretes MI support into advance force main body and rear guard ● Integrates ECM into braekout to megnify surprise, enhance shock affect, and "freeze" enemy in place ● Sees ahead of advance force to maintain momentum to breeknut ● Providas combat information to unit conducting supporting attack	● Ensures continuity of IEW communictions vie aerial reley during breakout ● Uses ECM to "slow/freaze" enemy reinforcements ● Jams the control communications ● Provides surveillance and reconnaissanca for flanks and rear ● Coordinates coverage with higher IEW staff unit ● Provides CI support
Ra-establishas communications	● Reports all deep battle data to higher haadquarters	● Requests aerial/ground relays
Limits damage by nuclear or chemicel attack	● Increases MOPP level ● Locates and reports enemy NBC delivery systams	
Continues the defense	● Develops contingency plans	
Mainteins morale	● Counters rumors, subversion, sedition, and propaganda	● Ensures NBC readiness ● Takes action to minimize effects of EMP
Considers exfiltration	● Devalops intelligence reporting channels to exploit HUMINT in the breakout corridor ● Providas CI coverage for evacuated araas and CPs	● Provides continuous IEW support ● Provides countar-technical intelligence for destroyed equipment ● Provides wounded with EEFI ● Supports creation of diversions

THE BREAKOUT FORCE



IEW SUPPORT TO LINKUP OPERATIONS

ENCIRCLED FORCE COMMANDER	IEW SUPPORT
Coordinates plans for linkup.	• Shifts IEW control to linkup force. • Exchanges enemy situation data with linkup force. • Coordinates and fulfills linkup force PIR. • Provides IEW-unique logistic requirements. • Sees deep and develops situation for actions after linkup.
Supports the relief attack.	• Reports results of collection effort to linkup force. • Supports with ECM.
Coordinates subsequent actions.	• Coordinates subsequent actions.

CHAPTER 11

Rear Operations

A major principle of Soviet military doctrine is to disrupt an adversary's rear area through the use of agents, saboteurs, terrorists, special action and diversionary forces; attacks by maneuver units; and aerial and artillery fires. Attacks against rear area targets are carefully coordinated as an extension of close operations. The goal of such rear area attacks is to degrade friendly support and sustainment of close operations and to divert forces from it. These attacks also contribute to the demoralization of friendly forces.

Air-land battle doctrine counters this threat by fusing rear, close, and deep operations into one unified, coherently executed battle. Actions and decisions in all areas impact upon one another. Unity of effort is the foundation of success. Commanders responsible for conducting deep and close operations are also responsible for conducting rear operations. They allocate available combat, combat support, and CSS to achieve success throughout the entire depth of the battle area.

In any future conflict against a major enemy force, the rear area will be characterized by intense enemy activity whose intent is to create panic and disruption. The objectives of enemy forces in the rear area are to—

- Destroy nuclear-capable delivery systems, headquarters, logistical installations, and nuclear storage sites.
- Disrupt rear area C^3 centers, airfield operations, and air warning and air defense systems.
- Neutralize high-ranking political and military personalities.
- Harass supply lines and disrupt lines of communication movement by seizing or destroying rail and highway junctures, key bridges, tunnels, defiles, and flood plain gates.

AIR-LAND BATTLE TENETS

Rear operations will be fought using the basic tenets of the air-land battle. They include—

- Initiative—to aggressively deny the enemy landing areas, to restrict access to critical bases, and to ensure continuous logistical support.
- Depth—to ensure a distribution of support so that close operations are not dependent on only one facility or storage area to continue the fight. To plan for alternative support and be prepared to shift that support without interruption.
- Agility—to anticipate and react to any rear threat by preparing and moving the necessary forces to meet and destroy the threat at any level throughout the width and depth of the rear area.
- Synchronization—to simultaneously sustain combat support and CSS of close operations and to coordinate combat assets to neutralize the rear threat without degradation of forward support.

Rear operations are defined as those actions, including ADC, taken by all units (combat, combat support, CSS, and host nation) singly or in a combined effort, to secure the force, neutralize or defeat enemy operations in the rear area, and ensure friendly freedom of action in the rear area.

ADC includes those measures taken before, during, and after hostile action or natural or man-made disasters to reduce the probability of damage and to minimize its effects.

OBJECTIVES

The objectives of rear operations are to—

- Secure the rear areas and facilities.
- Prevent or minimize enemy interference with C^3.
- Provide unimpeded movement of friendly units throughout the rear area.
- Find, fix, and destroy enemy forces in the rear area.
- Provide ADC before, during, and after an attack or natural disaster.

THREAT

Although rear operations have worldwide applicability, the threat to NATO is presented here as an example.

The Soviets will conduct operations in the enemy's rear area as part of their overall operations. Operations in the enemy rear area will support current (and prepare for future) operations. These activities in the rear area are designed to create fear, panic, and confusion among the civilian population, and to disrupt CSS operations throughout all echelons of their enemy's rear area through independent activity or operations that support efforts in the close operations.

LEVELS

Three levels of activity provide structure for and describe the threat. They serve as a guide when planning rear operations. They are as follows:

- Level I - Activity of enemy-controlled agents, sabotage by enemy sympathizers, terrorism.
- Level II - Diversionary and sabotage operations conducted by unconventional forces. Raid, ambush, and reconnaissance operations conducted by combat units. Special missions or UW missions.
- Level III (battalion-sized or larger) - Heliborne, airborne, amphibious, ground force deliberate, and infiltration operations.

These threat activities will not occur in a specific order nor is there a necessary interrelationship between threat levels. The rear area may face one or all actions at any given time, and in some cases, level I or level II activity will be conducted in support of a level III incursion or a major attack occurring in close operations. Additionally, some activities may take place well ahead of general hostilities, including terrorist attacks against key personnel and activities.

Other Soviet actions that may occur in the rear area include fires, floods, conventional and NBC artillery fires, aerial bombing, and missile attacks.

Level I

Activity of Enemy-Controlled Agents. Soviet UW operations are supported by agent networks in the target country. The KGB and the GRU recruit agents in vital social sectors of the target country. Current estimates of the number of agents located in NATO countries who are controlled directly or indirectly by potential enemy intelligence and security organizations exceed 20,000. Their primary missions include, but are not limited to, espionage, interdiction, and subversion. Some agents are employed in a passive role as sleepers during peacetime, but their activities are keyed to a buildup in preparation for war. Agents are scattered throughout the theater of operations. Concentrations of agents can be anticipated around key military, military-industrial, communications, and transportation centers.

Sabotage by Enemy Sympathizers. Substantial numbers of civilians are sympathetic to the enemy. Though they are not part of the organized agent structure, they will constitute a significant threat to the rear area. Sympathizers will be difficult to neutralize because their activities will be random and unpredictable. Some of their actions include arson, assassination, sabotage, and the theft of supplies and materiel. Their activity could also extend to political demonstrations which could create civil strife in the host country. This activity should be closely monitored for a link to enemy sympathizers.

Terrorism. Terrorist organizations are groups whose goals are to overthrow a government or economic structure by hostile force. Their actions are defined as criminal acts, often symbolic in nature, intended to influence an audience beyond the immediate victim. Terrorists instill fear by violence or threats of violence to obtain political, religious, or ideological goals. During the preparation for war and at the outbreak of hostilities, terrorists will take advantage of these economically and politically stressed situations. Their actions will be directed against the government or its economic symbols such as large corporations, military facilities, government agencies, and key military and civilian leaders. Many terrorist organizations have a Marxist-Leninist philosophy, so it is presumed that these organizations will assist Warsaw Pact forces. Also, there are independent terrorist cells whose actions will be difficult to analyze or predict.

Level II

Diversionary and Sabotage Operations Conducted by Unconventional Forces. The Soviets maintain highly trained special purpose forces under the GRU, known as SPETSNAZ. These forces will be introduced into the target countries before the actual outbreak of hostilities. These forces are manned by skilled officers, warrant officers, and senior NCOs operating in 5- to 12-man teams. They are adept at demolition, communications, and foreign weapons. Generally, some team members are fluent in the appropriate foreign language (for example, German or English) and are trained to imitate the culture of the infiltrated area.

There are various methods of insertion for these teams, including air-drop, helicopter, vehicles, foot, or by sea. They may wear NATO uniforms or civilian clothes, and their mission will be to conduct reconnaissance and possibly to disrupt or destroy critical military targets and installations in the rear area. Their primary targets follow the same mission profile as all the rear threat units:

- ☐ Nuclear weapons and their storage sites.
- ☐ C^2 facilities.
- ☐ Major logistic facilities.

SPETSNAZ forces are oriented against very specific targets. Depending on the situation, these forces may attack targets of opportunity. There is a SPETSNAZ brigade assigned to each front during wartime. Each Soviet fleet also has a naval SPETSNAZ brigade. These main SPETSNAZ forces may be employed in a joint operation by all army fronts in a unified effort.

Raid, Ambush, and Reconnaissance Operations Conducted by Combat Units. Each Soviet motorized rifle and tank division has a reconnaissance battalion, and each motorized rifle and tank regiment has a reconnaissance company within its force structure. The reconnaissance battalion will conduct reconnaissance and provide intelligence on enemy troop disposition, to include the enemy rear area.

The reconnaissance battalion normally employs itself in squad elements. It may have six to eight separate armored reconnaissance squads which consist of two to three BRDMs, BMPs, motorcycles, and medium tanks. The division reconnaissance battalion has an operational depth of some 50 kilometers (conventional) to 100 kilometers (nuclear) ahead of their parent organization. This unit is capable of conducting reconnaissance probes on three or four axes.

Specially organized reconnaissance groups may be directed to raid installations or to conduct ambushes, although their primary mission is to collect information. They can also be directed to locate specific reserves and to identify boundaries between units. These groups may also conduct specific missions, such as the capture of prisoners or documents or the surveillance of unit positions or movements.

Special Missions or UW Missions. These operations are conducted by either parachute or helicopter assault forces (company-sized or smaller) that are organized for reconnaissance or tailored to conduct sabotage or raids. Their missions include target reconnaissance and intelligence collection. They may attack nuclear delivery means and they may attempt to disrupt C^2 assets

and logistic facilities. These forces will harass units throughout the rear area. This mission may be used to assist level III threat forces.

Level III

Heliborne Operations. The Soviets possess dedicated heliborne forces. Doctrinally, these forces are employed to a depth of 50 kilometers and normally will be battalion-sized or smaller. The Soviets will attempt to keep the insertion within range of Soviet artillery and will also try to linkup with the heliborne force in a few hours. Selected motorized rifle battalions are also trained to conduct heliborne operations supported by army or front helicopter regiments.

Because of the number of helicopters required to lift a motorized rifle battalion and the weight restrictions of the helicopters, most of these operations are conducted without light armored vehicles. A battalion heliborne force could contain 500 troops. Typical heliborne missions are normally terrain-oriented but may be tailored to attack C^2 elements or communication facilities. Additional missions suitable for the heliborne force are ambushes, raids, sabotage, and laying or clearing minefields in the enemy rear area.

Airborne Operations. The Soviet Union maintains an elite force of paratroopers. The Soviets will employ airborne assets on both conventional and nuclear battlefields. Airborne forces are used to project combat power deep into the enemy rear area. The airborne insertion may support the rapid advance of a large combined arms force (operational maneuver group (OMG)) that may be attacking into the enemy rear area. These airborne forces can be dropped with their armored vehicles, the BMD airborne infantry fighting vehicle, and the ASU 85 assault gun. Soviet doctrine describes four types of airborne operations:

- Strategic airborne assault. This is a deep strike that will have a significant impact on a war or campaign. Some strategic objectives are national capitals, administrative and political centers, industrial and economic centers, and major airports and seaports.
- Operational airborne assault. This is a battalion-, regiment-, or division-sized airborne assault conducted in support of a front offensive in which a linkup would occur in several days or less. This mission would strike such key targets as bridgeheads; theater, army, group, or corps headquarters or CP; airfields; or river crossing sites.
- Tactical airborne assault. This is a shallow tactical assault, controlled at division level, normally against a specific objective. It is conducted by a reinforced company or battalion. This tactical assault is directed against enemy nuclear weapons and delivery means, CPs, logistic facilities, communication sites, and airfields.
- Special airborne operations. A special airborne mission is established by the Soviet Supreme High Command and controlled by front and army commands. This mission is conducted at the operational level or as directed by the KGB. The mission will be a sabotage or reconnaissance mission and will be conducted by a company-sized or smaller unit. The UW mission will be directed against a specific target to destroy nuclear delivery means, or, through demolition, arson, or flooding to destroy or deny the use of critical facilities. These special missions can also be conducted for PSYOP to spread rumors and to create panic, thereby disrupting the rear area.

Amphibious Operations. Soviet naval forces have initiated extensive training and development of their naval infantry. Recent developments indicate a definite enemy seaborne threat against critical US and other western rear area ports and facilities. The Soviet naval infantry has the capability to conduct tactical landings with highly mobile forces, air-cushioned vehicles, and high-speed landing ships. The Soviets categorize amphibious operations as follows:

- Strategic landing—multidivision landing with naval and air support to open or expand a military operation.

- Operational landing—a regiment- or division-sized landing to seize an island, a base, or a coastal facility.
- Tactical landing—a strike of battalion size or larger against an enemy coastline or facilities. This operation may be conducted in support of an inland group force operation.
- Reconnaissance and sabotage landing—a landing conducted by a battalion, company, or platoon against coastal facilities.

Ground Forces Deliberate Operations. The threat may attack units in the rear with an OMG. An OMG is generally a high speed, tank-heavy, operational exploitation force, separate from the second echelon. The mission of an OMG is to conduct operations deep into the enemy rear as early in the offensive as possible. The OMG is to destroy enemy nuclear weapons, C^3, and air defense; seize or disrupt lines of communications and airfields; and assist in the advance of main forces by seizing bridgeheads, road junctions, and so forth.

At front level, an OMG could be as large as a tank or combined arms army consisting of two to four divisions reinforced with airborne or air assault forces, aviation, artillery, air defense, engineer, and logistical elements. An OMG could be committed well before the front's immediate objective (enemy corps rear) is attained by first-echelon forces, normally on day 2 or 3 of the offensive.

An OMG at army-level probably would be as large as a reinforced division and could be committed as early as the first day of an operation. If the OMG is operating on the main axis of advance, the second echelon may be required to destroy forces bypassed by the OMG or to secure the OMG's lines of communications. Mission objectives could be nuclear weapons, withdrawing troops, reserves, C^3, logistics bases, or key terrain.

Infiltration Operations. Dismounted infantry forces may attempt to infiltrate battalion-sized and larger units into the friendly rear area. The unit will infiltrate as small elements through the main battle area and assemble at a key terrain feature at a designated time.

SUPPORTING FORCES AND TECHNIQUES

The Soviet Air Force will provide attack helicopters, ground attack aircraft, and fighter bombers in support of heliborne and amphibious operations. They will attempt to destroy air defense systems that defend a corridor into the rear area. This is a critical step in gaining air access for a level III incursion into the rear area.

Soviet combat helicopters (HAVOC/HIND/HIP) will be employed in support of offensive operations (airborne or heliborne) in the rear area. The armed helicopter will also conduct armed reconnaissance in the rear area. Helicopters will attack missiles being transported or in firing positions, C^2 facilities, and air assets on the ground. They will also conduct raids and ambushes. Attack helicopters will operate in teams of two to four helicopters. The plan is to attack after artillery preparations.

The FROG, SCUD, SCALEBOARD, SS-21, and SS-23 can deliver high explosive chemical or nuclear warheads at ranges from 70 to 900 kilometers. They are targeted against nuclear-capable artillery, rockets, control systems, CPs, radar stations, reserves, combat support, and CSS areas.

Mines provide another system for disruption of the rear area. Antipersonnel and antitank mines can be delivered by vehicles, aircraft, artillery, or individual soldiers. The mines will be used to isolate facilities, deny avenues of approach, and to restrict forward support.

The Soviet concept of REC integrates EW with artillery, rocket fire, and air operations. Tactical EW reconnaissance elements, both on the ground and in the air, will follow closely behind advancing regiments. These units will use SIGINT, DF, jamming, and deception against our forces. The goal of REC is to disrupt and destroy C^2 elements, radars, communications centers, and nuclear delivery means. Tactical missile systems will support REC targeting to a depth of more than 200 kilometers.

Additional information on Soviet threat forces can be found in FMs 100-2-1, 100-2-2, and 100-2-3.

COMMAND AND CONTROL

Rear operations are a command responsibility. Several key players are involved:

- ROO
- G3.
- Rear area operations center (RAOC).
- Security, plans, and operations and security, operations, training, and intelligence (SPO/SOTI) officer.
- MPs.
- Engineers.
- Base or base cluster commander.

The ROO will be appointed by the echelon commander based on the factors of METT-T. The ROO is responsible for the C^2 of rear operations and has control of all RAOC operations. The G3 or DCSOPS receives operational planning and support from the RAOC to conduct rear operations. The RAOC is the tactical center of the rear CP that controls rear operations at each echelon. In each echelon support command, the SPO/SOTI officer provides planning and control of all logistical distribution.

The MPs provide the combat link of rear operations. Their employment throughout the rear area provides the commander with a light, mobile force to affect rear operations.

The engineers are positioned throughout the battlefield and are given missions by the echelon commander depending on the situation. The base or base cluster commander will plan, prepare, and supervise internal defense for rear operations.

ROOs are physically located in their respective rear areas. The ROO will—

- Ensure that geographical areas of responsibility are clearly defined in the rear area.
- Use the RAOC to plan, coordinate, and direct rear operations.
- Be provided adequate, reliable communications equipment to facilitate C^2 of rear operations.
- Ensure close, continuous coordination between the G2, G3, and the RAOC.
- Coordinate with G5 and CA to integrate host nation support.

PRINCIPLES

Unity of Effort

This principle ensures the uninterrupted support of the main effort and the protection of the rear area. The keys to rear operations are sound planning, early warning, continuous OPSEC, and the rapid deployment of sufficient forces and resources to counter any threat. Rear operations are a command responsibility (brigade, division, corps, and theater army). Planning and execution will occur as part of the entire combat operation. The operation staff (G3, DCSOPS) will ensure that planning includes consideration for deep, close, and rear operations.

Economy of Force

This principle requires combat support and CSS units to defend themselves against attempts to disrupt their operations. They must be able to minimize destruction, reinforce their units, and defeat attacks or gain time until response forces arrive. They will form a base defense perimeter to defend against the threat. When enemy forces exceed base defense capabilities, MPs may provide the initial force to close with and destroy the enemy. If a threat exceeds the capability of units (MPs, CSS) in the rear area, combat forces will be assigned to rear operations to neutralize the threat. MPs and engineer units, respectively, are responsible to the ROO for rear operations.

Combat support and CSS commanders must be prepared to defend their units. Each establishes a base defense and provides a C^2 element for the base. This C^2 element is called a base defense operations center (BDOC). It is staffed and equipped by the host and tenant unit (or units) of the base. When a base comes under attack, outside response forces are not normally present. The base commander plans and directs base defense efforts with organic assets. The troops must be trained, equipped, and prepared to defend the base.

When units are grouped for security or emplaced for mission support, they will be formed into a base cluster for mutual support. The base cluster commander will establish a base cluster operations center (BCOC) for C^2 to coordinate rear operations among bases in close proximity to one another (distance will be dependent on terrain and mutual support). The BCOC will be staffed and equipped from units within the cluster.

The RAOC coordinates directly with the base cluster commander. The RAOC provides centralized tactical planning and control of rear operations. The RAOC will conduct direct staff coordination with the SPO, or with the SOTI of the echelon support command and the G3 or DCSOPS. The RAOC is under the operational control of the ROO.

The G3 assists in the integration of planning and execution of rear operations. Rear operations are integral to the overall operations, mission analysis, threat assessment, resource allocation, and base assessment of the echelon staff.

Detailed coordination is necessary between a host nation and the G5 to provide information and depth to security in the rear area. Interface between civil affairs teams or cells, CI teams, civilian police, and MPs aids in the efficent execution of rear operations.

The ROO reports directly to the echelon commander. The ROO controls rear operations through the RAOC and receives support from the G3. As the theater develops and more combat assets become available, the echelon commander may assign a tactical combat force to fight rear operations.

Responsiveness

This principle is key to defeating enemy incursions in the rear area. This involves the immediate reaction and rapid deployment of sufficient combat power and ADC resources to destroy the enemy and to minimize damage. Responsiveness is achieved through—

- ☐ Effective command relationships and command supervision.
- ☐ Reliable communications.
- ☐ Accurate intelligence.
- ☐ Centralized planning and decentralized execution.
- ☐ Organic mobility of response forces.
- ☐ Training and rehearsals.
- ☐ Prior assessment of the capabilities of bases and facilities to withstand enemy attack. This assessment is based on their degree of exposure and their importance as enemy targets. It assists the commander in allocating resources to protect personnel, supplies, and facilities in consonance with their importance to the mission.

TASKS

The base or base clusters will prepare their defense to accomplish the following tasks.

Secure Forward Support

Rear operations must secure and sustain combat support and CSS for forward combat units without seriously degrading the capability of the support command to accomplish its primary support mission.

Detection

Detection of the enemy is the responsibility of every soldier and intelligence collector in the command. Detection is accomplished by observation, reconnaissance, and surveillance during all weather and light conditions on any terrain. MPs aggressively patrol road networks and key terrain throughout the rear area. All personnel in the rear area provide information about any and all unusual or suspected activity.

The extensive use of active and passive measures to counter the enemy is mandatory. Detection means include the use of day and night observation devices, SIGINT assets, radar, REMS, and chemical and radiological detection equipment. These not only detect enemy infiltration attempts or the use of chemical or nuclear weapons, but also aid in preventing reactions to false alarms such as movements by friendly persons, defectors, or refugees.

Delay

Rear operations must sufficiently hinder the enemy's progress after detection to provide adequate time for friendly forces to react. This is done by establishing a base of fire and by employing mines, boobytraps, wire, or other obstacles to slow, impede, or canalize the enemy's movement. Scatterable mines make an effective rapidly-emplaced obstacle system. After infiltration attempts have been detected along existing or reinforcing obstacles, scatterable mines can be used to block the enemy's withdrawal, to restrict his lateral movement, or to strengthen the obstacles.

Destruction

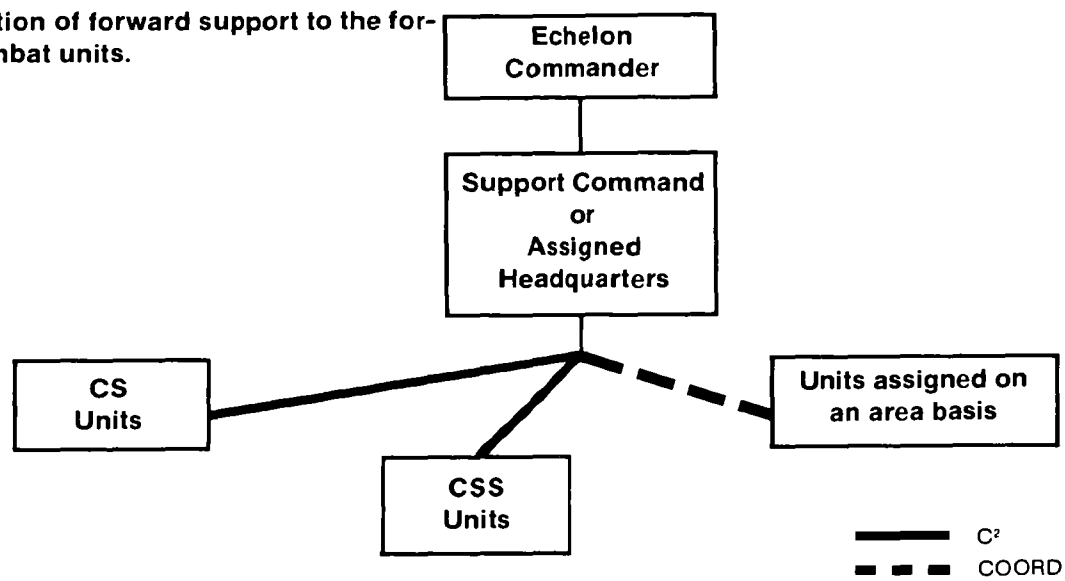
After the threat is detected and delayed, the enemy must be destroyed as quickly as possible. This is accomplished by air, land, or sea forces that kill, capture, or repel the enemy with all appropriate available firepower and manuever resources.

CHAIN OF COMMAND

The technical chain (see the following illustration) continues to function (performs combat support and CSS missions) until a threat requires a response by the base or base cluster commander. At this time, the base or base cluster commander uses the tactical chain of command (the RAOC) to defend his base. (See illustrations on pages 11-9 and 11-10.) The RAOC immediately notifies the SPO/SOTI, who, in coordination with the materiel management center (MMC) and the movement control center initiates coordination with other support elements outside the threatened area to ensure mission support provided from the attacked base or base cluster can be sustained from another location.

TECHNICAL CHAIN OF COMMAND

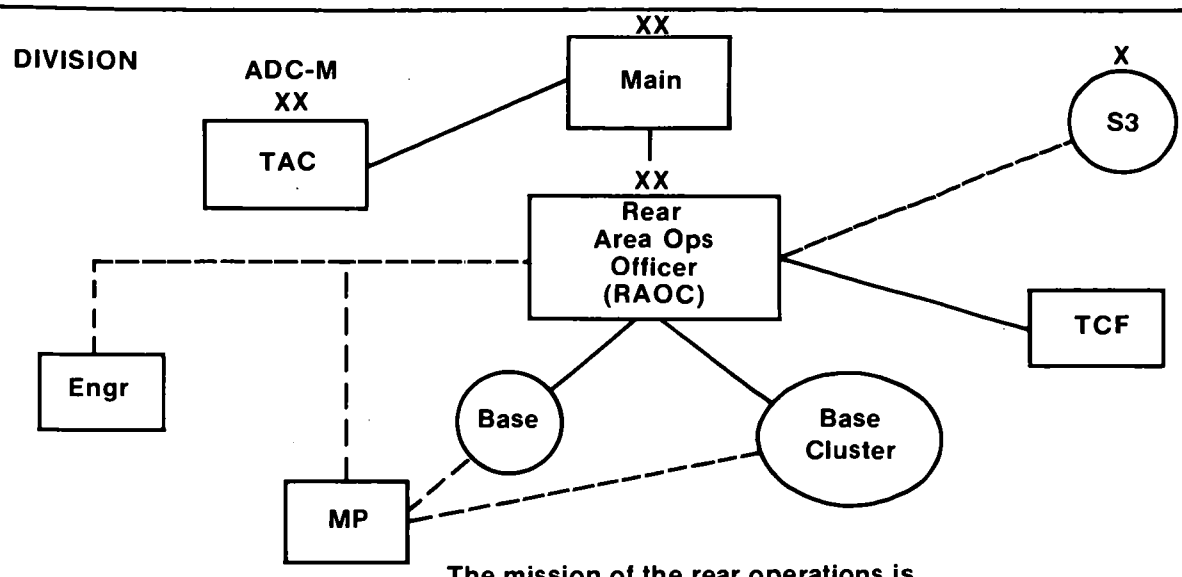
The technical chain of command controls all CS and CSS units. It ensures the continuation of forward support to the forward combat units.



ORGANIZATION

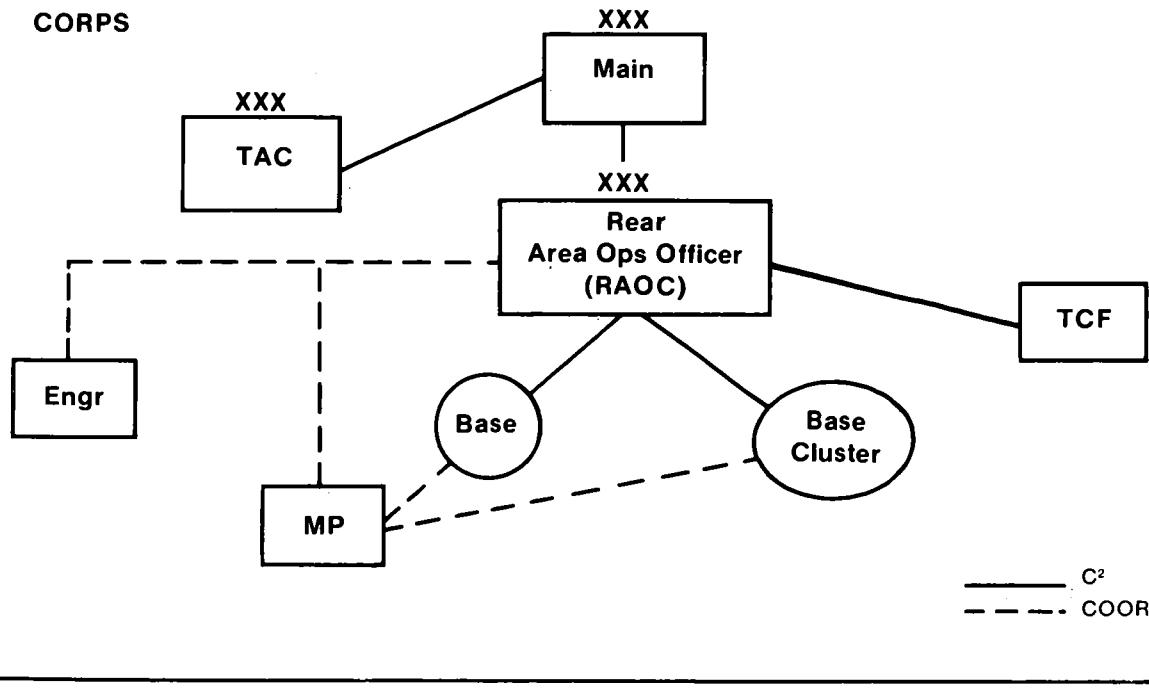
The RAOC is a tactical operations center whose organizational size will vary, based on geographical responsibility, the echelon it supports and the number of support units within the support area. The RAOC will be

DIVISION TACTICAL CHAIN OF COMMAND FOR REAR OPERATIONS



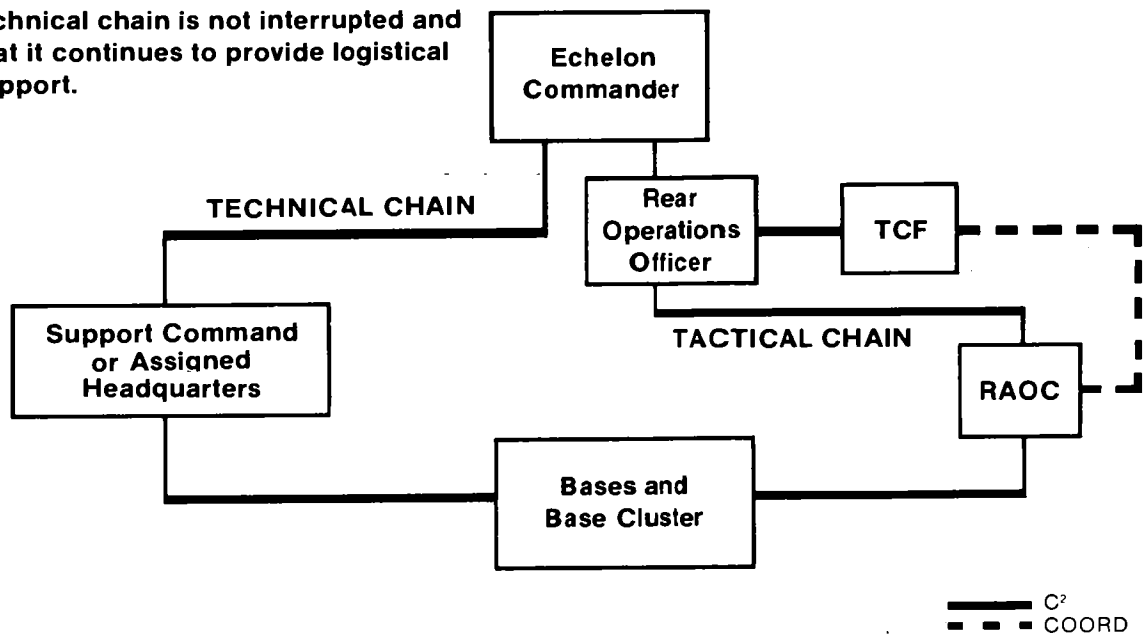
The mission of the rear operations is accomplished through the tactical chain of command.

CORPS TACTICAL CHAIN OF COMMAND FOR REAR OPERATIONS



THE COMBINED RELATIONSHIP OF THE TACTICAL AND TECHNICAL CHAIN OF COMMAND

Another primary mission of the tactical chain of command is to ensure that the technical chain is not interrupted and that it continues to provide logistical support.



centrally located within its AO. All RAOCs will normally position with the assigned ROO to enhance coordination. The RAOC is within the rear CP. The RAOC will act as the tactical center of the rear CP under the control of the ROO who may also control the rear CP. This relationship is the conduit for direct coordination with the main CP.

RESPONSIBILITIES

Based on echelon priorities and plans, the RAOC plans, coordinates, advises, and directs the execution of rear operations. As the tactical operations center for fighting in the rear area, the RAOC responds to the requirements of the echelon ROO.

The RAOC, in the execution of rear operations, will assist in the positioning of units in the rear area through the G3. The RAOC will designate the senior officer within each base as the base commander, who in turn will establish a BDOC. The RAOC will also cluster bases for mutual support. The base cluster commander will establish BCOCs. The base commander or base cluster commanders report directly to the RAOC to form the tactical chain of command for rear operations. The RAOC is responsible for the establishment of the tactical communications net to support the rear operations plan. The RAOC commander will coordinate with the echelon signal officer or unit to ensure that sufficient communication assets are available for bases or base clusters and alternative means of communication are available. When bases are so positioned that direct communications are not available, the RAOC will coordinate with the MPs to augment the rear operations (tactical) communications net. The MPs can provide this assistance through their organic communications and mobile patrols.

The division RAOC is the tactical operations center for rear operations in the division. The division RAOC will use base defense liaison teams (BDLTs) to coordinate with the S3s of the forward brigades. The ROO will appoint base cluster commanders as area commanders when the geographical area exceeds the capabilities of the RAOC. If area commanders are appointed in the division area, a BDLT will be attached as a staff augmentation to that area commander to assist in coordination of that geographical area.

The corps RAOC has responsibility for rear operations in the corps rear area. This RAOC provides missions to the MPs, engineers, and explosive ordnance disposal (EOD) control center in support of rear operations. The RAOC also provides a BDLT to the corps G3 and coordinates directly with the MP brigade, engineer brigade, and host-nation assets within the corps area. It also has direct access to the corps G2 for intelligence information and planning.

The corps support group (CSG) RAOCs are management centers for the corps RAOC. The CSG RAOCs will coordinate with all base clusters in the support group. The CSG RAOCs will also submit mission requests for MPs, engineers, and EOD support to the corps RAOC. MP and engineer assets are so austere that commitment of these assets at support group level would piecemeal these assets. The corps RAOC has the full perspective of rear operations and can request assets in the best interest of the corps. The corps RAOC BDLT will assist CSG RAOCs on an area basis.

The theater army RAOC (TA RAOC) is a staff element for coordination and control of rear operations. The TA RAOC, located near the TA DCSOPS, coordinates with the host nation and RAOC of the Theater Army Area Command (TAACOM). The TA RAOC provides directives from the TA commander.

The TAACOM RAOC exercises the same control relationship as the corps RAOC. However, because of the size of the TAACOM area, the TAACOM area support group RAOC coordinates mission requests for engineer, MP, and EOD assets directly with the units operating in the area support group (ASG).

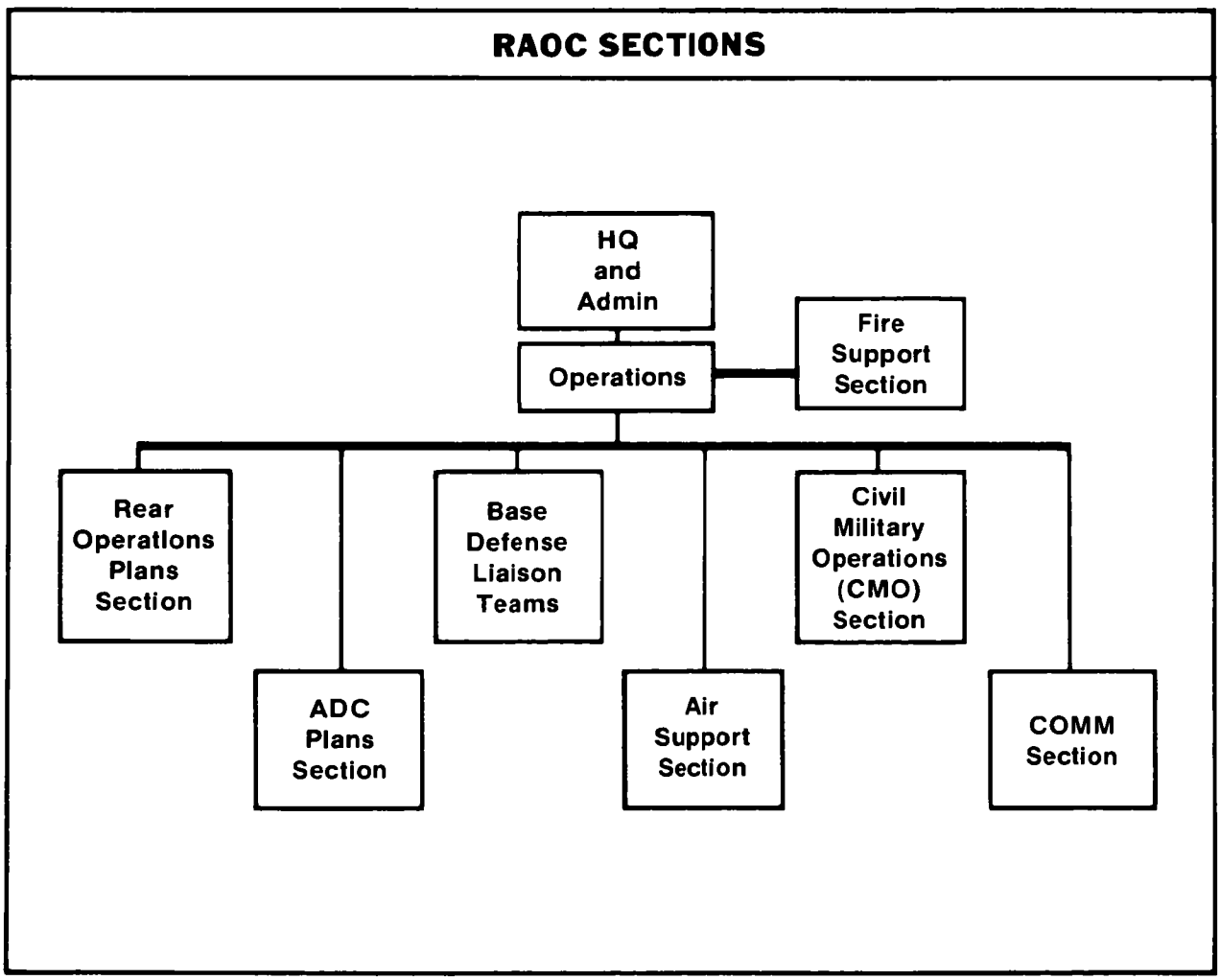
The ASG in the TAACOM will request support from assets in the TAACOM. The ASG RAOC will request support from the MP and engineer brigades for rear operations.

Though RAOCs are organized differently at each echelon, basic responsibilities are inherent to each section. The smaller RAOCs that do not have some sections (division RAOC, CSG RAOC, TAACOM RAOC) have personnel (for example, artillery officer or ordnance officer) within the organization who perform these tasks or obtain specific support from other echelon organizations (see the following illustration).

The sections within the RAOC have the following responsibilities. The headquarters and administrative section coordinates all personnel, administrative, and logistic support as required for the RAOC. The operations and intelligence section—

- ☐ Receives, correlates, analyzes, and reports the rear situation to the G3 and base clusters.
- ☐ Develops PIR and IR for the G2 to assist intelligence collectors in gathering intelligence for rear operations.
- ☐ Receives intelligence and information from the BDLT and reports it to the G2. Receives analyzed intelligence and information from the G2 and applies it to rear operations.
- ☐ Receives IPB products from the G2 and applies them to the intelligence preparation for rear operations.
- ☐ Receives and distributes air defense alert status from the ADA brigade.
- ☐ Receives base defense plans and develops operational plans for tactical combat forces (TCF) or other forces employed in support of rear operations.
- ☐ Receives requests from BDLTs and directs assets under control of the RAOC or requests assistance from the G3.

- Coordinate directly with the G3 and SPO/SOTI on critical bases, passing units, and moving of units. The RAOC will accomplish all support command coordination through the SPO/SOTI.
- Coordinates Air Force support through the Air Force liaison officer attached to the RAOC.
- Coordinates the positioning of critical supplies in the rear and makes recommendations for critical bases determined by the logistics available at each echelon.
- Coordinates with the SPO/SOTI on all movement of bases or units into the RAOC area of responsibility.
- Initiates the request for a TCF to be employed in the rear and provides guidance as to tactical boundaries, units under the OPCON of the TCF, and mission requirements.
- Monitors and supervises the communications data distribution and tactical computer systems and coordinates required support for the system.
- Coordinates automation requirements for the RAOC.
- Coordinates training of base defense units with the appropriate unit or staff.
- Maintains rear operations pattern analysis files, conducts pattern analysis, requests additional MI assets, and adjusts its collection plan to support pattern analysis.



Tactical Combat Force Support

The TCF is a combined arms organization assigned to fight rear operations. This may be a unit reassigned a RAOC mission from close operations or initially assigned to the rear. Any echelon may create a TCF and attach this tactical unit to the RAOC to fight rear operations. The TCF will be task organized by the G3 to defeat the threat. It may have supporting artillery or aviation support as task organized by the G3.

When the TCF is employed for rear operations, they will use their organic CEOI. The BDLT as the coordination element will operate with the TCF S3 or G3 and provide liaison and direct communications between the TCF and the RAOC. If additional support is required, the rear operations net can be used to expand support through the area signal system. The MP assets OPCON to the TCF will provide an additional back-up communications capability.

When the threat in the rear area exceeds the capability of the MP and base defense forces, the RAOC will notify the ROO that a TCF is required. The ROO will notify the echelon commander. The G3 will analyze the situation with other staff elements and will make one of the following recommendations to the commander:

- ☐ Direct MP and reaction forces to harass and delay to gain time.
- ☐ Provide direct or indirect fire systems to weight the battle for the MPs.
- ☐ Commit assets from close operations.
- ☐ Request a TCF from a higher headquarters. (Depending on the tactical situation, a TCF may have been assigned to rear operations. In this case, the ROO will have the authority to commit this force.)

If the MPs are tasked by the G3 to delay the force, the MP commander (provost marshall, MP brigade commander) will become the response force commander. The MP commander will consolidate MP assets and execute a delay using MP assets and any other available force under the control of the RAOC. Assets committed to support the delay will be under the OPCON of the MP commander.

Artillery for Rear Operations

When artillery is committed to weight rear operations instead of a TCF, the artillery unit may be in DS of the RAOC, the MPs, or a unit directly involved in rear operations. The FSE or artillery officer of the RAOC will provide the artillery unit with the overlays and disposition of forces in the AO. In coordination between the RAOC and the artillery unit, control measures will be established. A restricted fire area may be established around each base or base cluster as required to support fires for the MPs.

If forward observers are not available, the MPs, base cluster commander, or an appointed individual in the AO may act as the forward observer for the artillery unit. The RAOC will coordinate with the SPO/SOTI who will assist in establishing the necessary logistic support for the artillery unit while it is in support of the RAOC. If the TCF is still required after the introduction of the artillery unit, the artillery unit may revert to the support of the TCF on order of the RAOC.

G2/Intelligence

The RAOC must generate requirements for intelligence collectors. The RAOC is a consumer of intelligence. The RAOC must ask questions of the G2 or echelon TOC support elements so that the G2 can identify collectors to assist the RAOC intelligence officer. The RAOC must assume the initiative in this area. Requests for overflights of the rear area and CI teams to operate near built-up areas and industrial facilities are part of the RAOC responsibility for developing the intelligence for rear operations.

Counterintelligence

Early coordination with CI teams through the G2 aids the RAOC in identifying and reducing possible level I threats in the rear area. The CI teams coordinate with local police, government officials, and counterterrorist organizations. CI teams provide invaluable sources for intelligence to predict and identify levels I and II threat activity. The CI effort is a continuous long-range

operation which will provide sources of information to the RAOC. See FM 34-60 for a detailed discussion of CI support to rear operations.

G5/Civil Affairs

Civil affairs (CA) units will be operating in and around the rear area. They operate from the forward brigade area through the communications zone. The coordination and assistance they provide are critical to the development of host nation support. During their work, CA elements will often gain information critical to the discovery, control, and neutralization of level I and some level II threats. The MP and CA teams will share this type of information through mutual support. The ADC plans section can also use the CA teams to locate and identify host-nation assets for ADC support.

INTELLIGENCE MISSION

To conduct rear operations successfully, the echelon commander and the ROO must know enemy capabilities and intentions. They must anticipate enemy actions and receive early warning of incoming incursions in the rear area. Therefore, the all-source intelligence mission in support of rear operations is to provide echelon commanders with timely and accurate intelligence regarding rear operations. This mission requires the following:

- ☐ Integration of intelligence from all sources at all echelons.
- ☐ Exchange of intelligence between US, host nation, and allied forces.
- ☐ Provision of OPSEC support to US combat, combat support, and CSS elements in the rear area.
- ☐ Dissemination of all-source intelligence and combat information in a timely manner.

A critical intelligence task in support of rear operations is to determine when and where enemy airborne or airmobile forces may be committed. Since these forces stage and deploy from areas beyond the corps area of interest, the corps is highly dependent upon EAC for early warning.

The RAOC intelligence officer is the interface into the intelligence system. The rear operations intelligence system is dependent on division, corps, EAC, and allied and host-nation intelligence collection, processing, and dissemination systems. These must be exploited through all available means.

RESPONSIBILITIES

Rear Area Operations Center

The RAOC is the focal point for the collection and dissemination of all rear operations intelligence. The ROO uses this information to allocate and position rear operations forces and to evaluate the positioning of critical bases.

G2/DTOC Support Element/ CTOC Support Element

The support element provides analysis and fused intelligence (including IPB) on probable enemy courses of action directly to the RAOC at each echelon.

MI Brigade (CEWI)

The MI brigade at corps supports rear operations as part of its mission. This mission is carried out, in response to G2 priorities, principally by the MI brigade along with indigenous security, CI, and police agencies on matters relating to rear operations (countersabotage, counterespionage, countersubversion, and terrorism). The MI brigade also supports rear operations through the following:

COMINT. The brigade will employ COMINT systems that can intercept and locate enemy HF and VHF communications in the rear area.

Weather support. Tactical weather support is provided by the USAF SWO and the USAF weather team (WETM). Weather information allows the commander to assess the effects of weather on weapons systems and tactics.

Intelligence preparation of the rear area. This continuous process develops a comprehensive and accurate data base of weather, enemy, and terrain information from all available sources before and during hostilities. This information, when integrated and analyzed with other intelligence

before and during hostilities, is the key to determining level III threat targets, landing sites, and air and ground avenues of approach. It enables the echelon commander to determine his vulnerable areas, analyze the threat, upgrade facilities and procedures as necessary, and prepare contingency plans. The same methodology and analytical approach applied to the intelligence preparation of deep and close operations also applies to the IPB for rear operations. This analysis extends past the echelon commander's area of operations into his area of interest.

An important aspect of this process is the preparation of the templates that analysts use to postulate and graphically portray enemy capabilities, vulnerabilities, intentions, and courses of action. The RAOC will need doctrinal templates of enemy airborne and heliborne DZ and LZ configurations, as well as of battalion and regimental operations once on the ground.

Target development. This process provides targeting information to the ROO based on the commander's base assessment. It involves cueing intelligence assets to provide accurate and timely detection, identification, and location of enemy activity and HVTs in sufficient detail and in time for effective attack. An example of a high-value rear area target for attack helicopters, close air support aircraft, and artillery would be an enemy airmobile battalion on an LZ.

Situation development. This process provides information that enables the commander to see rear operations in sufficient time and detail to generate the appropriate force at the right time and place. Situation development includes a detailed analysis of the weather, terrain, and enemy capabilities based on intelligence from all sources and provides the basis for projecting enemy intentions.

Collection management. Through integrated management, intelligence collectors interface with, cue, and complement other collectors at each echelon and within the national intelligence structure to satisfy PIR and IR.

EW support. EW planning and support are provided to the RAOC to electronically degrade or disrupt enemy C^2 communications. Requests for EW support from the RAOC are directed to the appropriate EW section (electronic warfare support officer within the corps G3 section).

OPSEC support. OPSEC support provides the commander with the ability to see himself through the eyes of the enemy commander. The OPSEC data base identifies enemy intelligence capabilities and friendly unit HVTs, patterns, and profiles. It identifies the vulnerabilities of friendly forces and recommends countermeasures. OPSEC support reinforces the commander's base assessment.

IMINT. SLAR, infared radiation, and photographic IMINT are provided to the RAOC upon request. IMINT allows the RAOC and TCF commanders to see the threat during periods of darkness and assists in assessing the OPSEC posture.

CI support. Besides being familiar with the hostile threat capabilities in the rear area, CI personnel are aware of the scheme of maneuver for friendly deployed units. They also know and understand the commander's rear operations plan.

Upgrading intelligence holdings from reports submitted by all sources plays an important part in providing an accurate picture of enemy intentions for rear operations. Because the rear threat is dynamic, CI personnel must continually assess the level of threat and develop and recommend appropriate countermeasures to frustrate or eliminate the threat.

Close liaison with police, civilians, MI agencies, the G5, and CA personnel is a daily function. When hostile rear area attacks begin, cooperation between agencies is critical in neutralizing the threat, particularly at level I.

Based on information on potential hostile rear area activity, DSO are established to provide leads for the identification of perpetrators of incidents against friendly units

and personnel. DSO are composed of personnel who serve as paid or unpaid informants. They are generally local national employees such as barbers, civil laborers, and others whose access to the military and civilian community may put them in a position to become aware of potential activities against friendly facilities.

INVESTIGATIONS

Incidents of suspected sabotage, espionage, or subversion are investigated by CI personnel as directed. These investigations can lead to identification and elimination of perpetrators of hostile actions in the rear area. Pattern analysis of multiple incidents can reveal enemy plans and intentions.

Black lists are created and updated to permit rapid identification of key suspects in the rear area. Persons on these lists are those personnel whose capture and detention are of prime importance to the US Army at or during the outbreak of hostilities. They include known or suspected agents, saboteurs, enemy sympathizers, and others who represent a serious threat to rear operations.

Identification and neutralization of hostile teams and cells are an important priority in rear operations. Information provided by CI personnel is passed to local police, MPs, or allied forces for action.

Tactical HUMINT operations are employed to exploit those captured personnel who can quickly identify other hostile agents and saboteurs and pinpoint unit or team locations, future plans, or weaknesses. Time constraints generally prevent extensive tactical HUMINT operations at level III, but enemy agents, sympathizers, and terrorists can often be neutralized at levels I and II.

CI personnel identify line crossers, refugees, or defectors who can provide critical information. In TA, this mission exists during times of war and peace and provides for medium- and long-range CI planning and activities. During war, CI teams located near or collocated with the corps EPW cage will have EPWs, refugees, defectors, and line crossers identified by interrogators as being of CI interest. CI personnel conduct interviews or interrogations of these individuals and are primarily concerned with CI information of current tactical value. Frequently, these interviews or interrogations require a joint effort by CI and interrogation personnel using the appropriate language.

MPs will frequently collect intelligence and information from US or host-nation sources while performing their mission in the rear area. The MP headquarters will disseminate this information to the RAOC via the existing communications net.

Examples of sources of information and intelligence to the RAOC for the three threat levels are as follows:

- Levels I and II:
  - MI battalion (TE).
  - CI teams.
  - Bases and base cluster S2s.
  - MP.
  - Convoys.
  - Civilian police.
  - Host and allied nations.
  - Special forces detachments.
  - Inflight reports from aircraft.
  - GSRs.
  - Remotely monitored sensors.
  - CA units.
- Level III:
  - EAC intelligence units.
  - MI battalion (TE).
  - Division MI battalion.
  - Air defense radars.
  - Air Force intelligence systems.
  - Combat units.
  - Inflight reports from aircraft.
  - Allied and host-nation units.
  - MP.
  - National systems.

INTELLIGENCE AND ELECTRONIC WARFARE SUPPORT

While the collection efforts of all IEW assets support rear operations through collection against enemy forces that pose a threat to the rear area, normally only CI assets will directly support rear operations against levels I and II threat. Some other IEW assets (EW, GSR, interrogation) will have, on order, missions to redirect their efforts from deep and close operations to rear operations to support combat forces against level III threat.

Additional information on rear operations is contained in FM 90-14.

CHAPTER 12

Special Operations and Environments

The geographic range of US interests demands that the Army be prepared to fight and win on all types of terrain and in all climates. This chapter describes IEW support to special operations and in special environments. Each operation or environment is described in general terms to establish a basis for understanding its impact on IEW operations. Special considerations for conducting and sustaining IEW operations are then described to aid in planning, organizing, and training for these operations and environments.

SPECIAL OPERATIONS

JCS Publication 1 defines special operations as operations conducted by specially trained, equipped, and organized DOD forces against strategic or tactical targets in pursuit of national military, political, economic, or psychological objectives. These operations may be conducted during periods of peace or hostilities. They may support conventional operations, or they may be prosecuted independently when use of conventional forces is either inappropriate or infeasible.

This chapter focuses on the MI aspects of air assault, airborne, riverine, amphibious, and LIC operations. Division operations are described, but the considerations given also may apply to smaller task force operations. These exceptions are noted where appropriate.

AIR ASSAULT

Air assault operations are characterized by a high degree of tactical mobility. They are conducted by transporting infantry and field artillery units, with the necessary combat support and CSS, into battle by helicopter. Once deployed on the ground, air assault infantry battalions fight like other infantry battalions. The essence of air assault tactics is a rapid tempo of operations over extended ranges. Air assault operations are described in FM 71-101.

Security of aircraft enroute to LZs is a major concern. Friendly air and air defense support must ensure air routes are free of enemy air and air defense forces. When REMS are available, friendly air assets seed likely enemy ground approach routes into the LZ with REMS to detect and report movement on the ground. GSR are employed to warn of enemy movement on friendly flanks.

Weather conditions may restrict the use of air assault forces especially when ceilings are below 200 feet and visibility is 1/4 mile or less. Adverse weather and natural and artificial obscuration hamper air and ground navigation, reconnaissance and surveillance, and resupply or extraction of committed forces. Sensitivity to weather factors guide the G2 during IPB and collection planning. Both current and predicted surface and aloft conditions are critical.

Terrain is equally critical. Terrain in the intended area of operations must be analyzed for its impact on the mission and the weapons and equipment required for the operation. Terrain in the objective area is analyzed to determine where the air assault force can obtain the best observation, fields of fire, and concealment and cover. Obstacles to air and ground movement and key terrain are identified. Key terrain for an air assault operation may include—

- Objectives of the assault and subsequent operations.
- Primary and alternate LZs.
- Emergency LZs enroute to the objective.
- Air routes in and out of the objective area.

Size and proximity to the objective and enemy forces are considerations for selecting an LZ.

Thorough IPB is required to give friendly forces detailed intelligence about anticipated friendly and enemy avenues of approach, LZs, and the area around the LZs. Barriers and obstacles must be located precisely.

Surprise is crucial to air assault operations which place forces in enemy held terrain. Therefore, OPSEC before and during the operation must deny the enemy information concerning the planned operation. In particular, OPSEC must hide indicators which would give the enemy knowledge of the—

- ☐ Intent to use air assault forces for a particular operation.
- ☐ Date and time of the operation.
- ☐ Size of the force to be used.
- ☐ Air routes to and from the planned LZs.
- ☐ Locations of the planned LZs.

Air assault operations require extensive CI support in both the preparation phase and the actual operation. CI analysis is critical to ensure OPSEC measures are taken to prevent giving away any of the information listed above. CI must also support actions at the staging areas to prevent espionage, sabotage, and acts of terrorism which could impact adversely on the operation.

Depending on the size of the operation, the first few hours on the ground are the most dangerous for air assault forces in areas under enemy control. If the enemy is able to react quickly and with sufficient force, the assault force can be defeated before its objective is achieved or before the bulk of its combat power and support can be consolidated and used effectively. In addition to OPSEC measures designed to deny the enemy information about the operation, other activities must be oriented toward preventing a thoroughly coordinated, rapid enemy response.

Deception measures are used for both purposes. Actions are taken to deceive the enemy about the operation and its purpose and to cause uncertainty and confusion in the enemy commander's mind once the operation has begun.

ECM also supports friendly efforts to stave off effective enemy responses to the operation. By jamming critical C^2 links, confusion and disorder can be created within the enemy command structure, prolonging the time required to organize and react.

MI personnel supporting the air assault force rely heavily on higher echelons for both intelligence and CI support to augment and reinforce organic capabilities. In some cases, depending on the size of the assault force, higher echelons must also provide additional EW support. Requests for information and requests for specific types of support are submitted as early as possible in the planning phase.

The MI unit commander supporting an air assault operation task organizes to meet the special requirements for mobility by helicopter. Generally, emphasis is on lightweight, manpacked systems for the initial assault. In the air assault division these include man-transportable, voice intercept systems in the low-level intercept teams and manpacked GSR. Vehicle mounted IEW systems may be lifted into the assault area after LZs are secured.

AIRBORNE

Airborne forces are organized to deploy rapidly anywhere in the world to—

- ☐ Secure critical installations or facilities.
- ☐ Reinforce US or allied forces.
- ☐ Conduct a show of force.
- ☐ Assault the enemy's rear area, secure terrain, or interdict routes of supply or enemy withdrawal.

Airborne forces are lightly equipped and, as a general rule, fight as light infantry once on the ground. To conduct sustained combat operations, they must be reinforced with additional medium artillery, air defense systems, and transportation.

Airborne operations are most often joint operations. Airborne forces are usually transported to the operational area by USAF aircraft although Army helicopters may be used in some cases.

Airborne operations require specialized information on the—

- ☐ Enemy composition, disposition, and strength in and near the projected AO.
- ☐ Enemy reinforcing capabilities.
- ☐ Enemy air defense capabilities.
- ☐ Weather conditions and seasonal peculiarities in the objective area.
- ☐ Weather conditions at the departure airfields and along the route to the objective area.
- ☐ Visibility in the objective area projected for the time of the assault and during follow-up operations.
- ☐ Key or decisive terrain.
- ☐ Primary, alternate, and potential emergency DZs.
- ☐ Routes into and out of the objective area for both enemy and friendly forces.
- ☐ Concealment and cover and fields of fire in the AO.
- ☐ Obstacles which inhibit or enhance airborne operations.
- ☐ Soil conditions in the objective area.

EW and CI support requirements for airborne operations are nearly identical to those of the air assault operation. However, in some cases, CI and EW support may be even more critical to the airborne operation.

Airborne operations often take place well beyond the range of MI assets supporting the airborne force. During planning for airborne operations, corps, EAC, other services, and national systems are the primary sources of intelligence. During the operation, organic resources provide much of the intelligence needed with additional support coming from the higher levels.

The MI commander supporting the airborne force task organizes MI resources to support every phase of the operation. Generally, MI units organic to airborne divisions are capable of accompanying combat forces on the initial parachute drop into the objective area. Those MI resources capable of functioning without extensive transportation or logistic support normally are the elements assigned to accompany the combat forces. The remaining elements of the MI unit and supporting elements from higher headquarters may be airdropped or airlanded after the immediate objectives have been taken.

Doctrine for planning airborne operations is contained in FM 100-27 and airborne division operations are described in FM 71-101.

RIVERINE

Riverine warfare differs from conventional ground warfare chiefly in environment. Environmental considerations have significant impact on the IEW support required for both planning and operations. Riverine operations are normally conducted jointly by Army and Navy forces.

Intelligence personnel coordinate through the J2 to achieve common objectives. Operations are jointly planned and decentrally executed. Riverine operations may include force insertion by watercraft, helicopter, parachute assault, and mounted or dismounted overland techniques.

The enemy's use of inland waterways and attempts to control friendly use of them demand special attention. The criticality of terrain intelligence and route reconnaissance in riverine operations places unusually heavy demands on IEW elements.

Significant contributions to the special environmental intelligence requirements can be made by combat engineer units. The following types of information are provided by these units:

- ☐ Width, depth, and bottom characteristics of waterways.
- ☐ Velocity and nature of current and tidal effects.

- ☐ Height, slope, and condition of banks.
- ☐ Location of natural and man-made obstacles.
- ☐ Location and gradient of possible crossing sites.
- ☐ High and low water underbridge clearance.
- ☐ Predictions of river stages during floods or heavy rains.

MI personnel modify standard IPB and collection techniques to accommodate the peculiarities of riverine operations. The following categories of information receive special attention for priority collection:

- ☐ Size and capabilities of enemy forces.
- ☐ Attitudes of local civilians.
- ☐ Descriptions of enemy-controlled congested areas.
- ☐ Presence, condition, and capacity of bridges in enemy controlled areas.
- ☐ Presence and use of mines, boobytraps, or demolitions.
- ☐ Presence of heavy vegetation and tree lines.
- ☐ Areas along and adjacent to waterways which are potential landing sites or zones for watercraft or air assault vehicles.
- ☐ Key terrain which offers excellent observation, fields of fire, and maximum grazing fire into a landing site or zone.
- ☐ Terrain which offers successive delay position opportunities.
- ☐ Location of trails and footpaths parallel to waterways.
- ☐ Movement of indigenous personnel to and from civilian activities.
- ☐ Presence and location of enemy and civilian signal, communication, and noncommunication systems.
- ☐ Enemy or civilian use of the electromagnetic spectrum.
- ☐ Alteration of waterway inlets which provide concealment for small watercraft.

The requirement to collect, process, and disseminate information and intelligence on the enemy, weather, and terrain is made more difficult by the riverine environment. The following factors inhibit effective IEW operations:

- ☐ Temporary or nonexistent security of land-based sites for sensor employment.
- ☐ Limitations placed on overhead platforms by overcast skies, ground fog, and heavy rain.
- ☐ Limitations placed on ground mobility by waterways, mud, lack of roadways, and uncertain cross-country mobility. These factors apply to the foot soldier and wheeled and tracked vehicles.
- ☐ Marginal effectiveness of GSR and night observation devices when operated from unstable waterborne platforms.
- ☐ Limited data from ground-based SIGINT or EW systems operating at reduced ranges. Accuracy of DF systems will be reduced due to vegetation and surface water.

Because of these limitations, heavy reliance is placed on aerial platforms. Aerial reconnaissance and SIGINT systems provide the most valuable, explicit intelligence and targeting information in a riverine environment. However, other sources, such as HUMINT, must not be overlooked.

The requirement to operate an IEW force in a riverine environment challenges the ingenuity of MI commanders, logisticians, and maintenance technicians. Ground-based prime mover and shelter configurations are modified to accommodate the environment. Early identification of suitable watercraft requirements is necessary to assure operational and service support capabilities. Shelter integrity is maintained where possible to facilitate position configuration and movement between waterborne carriers. Single position redundancy of electronic systems and power generation equipment is desirable. System components and operators must be shielded from small arms fire.

MI commanders task organize resources to sustain independent operations in remote locations for extended periods. Communications personnel are trained in manual Morse HF techniques in order to overcome or reduce the relative ineffectiveness of FM radios. Adjustment to one-time, pad-type encryption and decryption is made. Appropriate cryptomaterials are requisitioned through normal channels.

AMPHIBIOUS

Amphibious warfare integrates virtually all types of ships, aircraft, weapons, and landing forces in a concerted military effort against a hostile shore. The naval character of amphibious operations is reflected in the principles which govern the organization of the forces and the execution of the operations.

MI commanders and staffs should have a thorough understanding of FMs 31-11 and 31-12 prior to planning or executing amphibious operations. The joint nature of this type operation, and the unique intelligence and information requirements, make full knowledge of C^2 and coordination protocols an absolute necessity. Operations are jointly planned and decentrally executed.

Army IEW operations prior to an amphibious assault sometimes are hampered by the range to the target. Army IEW assets normally will not be operational prior to the operation nor while enroute to the objective area. This problem is overcome partially through thorough, detailed IPB before embarkation. Additionally, Army IEW staffs coordinate with Navy counterparts to maintain continuity on Army targets and areas of interest.

The desired objective is that there be no loss of continuity to Army IEW efforts while in transit. Heavy reliance on national systems and naval intelligence assets will be necessary until land-based IEW operations are established and fully functioning. PIR and IR of Army commanders are integrated with and communicated to the intelligence center of the JTF conducting the operation.

The following types of information are critical to Army participation in amphibious operations:

- Location, length, width, gradient, soil composition, and trafficability of beaches.
- Natural and man-made obstacles on and adjacent to beaches.
- Avenues of approach and areas of advance to and from the beachhead.
- Enemy beach defenses.
- Key terrain adjacent to beaches.
- Sea approaches including depth of water, underwater gradient, and offshore obstacles to include minefields.
- Surf, tide, and current conditions.
- Visibility.
- Winds.
- Light data.
- Precipitation.
- Height of breaking surf and deepwater waves.
- Temperature adjusted for wet bulb or windchill.
- Type, strength, and capabilities of enemy forces in the beachhead and objective areas and those that are capable of reinforcing.

The amphibious task force commander is responsible for the consolidation of intelligence requirements for the entire task force. Additional responsibilities include—

- Collection, processing, and dissemination of intelligence to major elements of the amphibious task force in accordance with the requirements of each.
- Acquisition and distribution of maps, charts, photographs, and special intelligence materials.
- Preparation of intelligence estimates affecting the entire task force.
- Preparation of intelligence studies which relate to the mission and AO.
- Establishment of liaison with operational intelligence agencies which are not part of the amphibious task force.

- ☐ Initiation of requests and directives for the collection of information.
- ☐ Security and CI measures.
- ☐ Preparation and distribution of an intelligence annex to the amphibious task force operation plan.
- ☐ Establishment of a target information center.
- ☐ Establishment of a JIC at the outset of planning in conjunction with the landing force commander as required.

The landing force commander assists the amphibious task force commander in the execution of intelligence duties and responsibilities. The landing force commander assists in the determination of the requirements for a JIC and provision of required representatives to staff the JIC.

Other force commanders are responsible for determining and stating their intelligence requirements and for preparing and executing an appropriate intelligence plan. Requests for intelligence peculiar to the specialized operations of these forces is submitted by the force commander to the amphibious task force commander through intelligence channels.

Once an amphibious plan is implemented, and the joint command becomes operational, the procedures for requesting and receiving information change. There are two major reasons for this. First, shared national resources focus capabilities on a centralized AO and become responsive to the mission of the JTF. Second, priorities for collection are established by the JTF J2. The result is more efficient processing and dissemination of intelligence. Although the process becomes more efficient, required intelligence details may become more obscure to the force commander due to the macro-nature of the products. It is, therefore, the Army G2 and G3 responsibility to anticipate contingency areas for likely joint amphibious operations, and to begin IPB and operations planning early. The JTF intelligence effort can then focus its reconnaissance and surveillance resources on updating or reinforcing data which is already held.

MI unit commanders are provided opportunities for sharpening the skills of their soldiers during the extended transit times of waterborne, surface movement. Training deficiencies and combat indoctrination concerning the enemy, weather, and terrain receive the top priorities. In-transit maintenance of equipment and physical fitness are emphasized.

LOW INTENSITY CONFLICT

LIC is defined by FM 100-20 as the use of military assets, in concert with other aspects of national power, by the national command authority to gain or protect its national objectives and interests. It may include the direct or indirect support of one or more foreign governments or groups, or be initiated as unilateral activities in the absence of such foreign support. Low intensity activities primarily focus on the use of power, and only on military force as a final alternative. Such activities can have limited or unlimited objectives.

LIC is a form of confrontation that has become a major concern of US policy. Since the Korean War there have been no high intensity conflicts involving major powers, but there have been hundreds of LICs. Historically, US involvement has been in response to an insurgency in a developing nation.

The IEW principles for the air-land battle apply equally well for LIC. The intelligence indicators for insurgent activity are, however, unique. Anything that insurgents can do to influence and direct a society toward overthrowing its government is reflected by some action or indication, no matter how subtle. As described in Chapter 3, the development and application of appropriate indicators is a key step in quantifying the collection effort.

US Army commitment in a LIC may occur suddenly or gradually over a period of time. The IEW staff, in coordination with the security assistance office and other members of the country team, assists in the development of the intelligence portion of contingency plans for US assistance. US support may consist of advice, financial

and material aid, provisions for professional education, and development of an intelligence documentary data base. Most of this effort is directed at the host-country national level, but mobile training and advisors may be sent throughout the country to subnational levels. Some MI advisors may be required to assist paramilitary and nonmilitary elements in developing HUMINT sources and exploiting the information they provide.

US military involvement in a LIC can shift rapidly from the advisory role to an operational role. Those already established intelligence functions would continue. Additional roles for intelligence elements in an operational environment may include—

- Population and resource control.
- Tactical operations.
- Combined MI operations with the host country in the form of interrogation, materiel and document exploitation, and imagery analysis centers.

LIC is the least studied of all potential conflicts, but has a high probability of US involvement in foreign political and military affairs. The US Central Command gives high priority to preparation for LIC contingencies. LIC peculiarities must be thoroughly studied by all MI personnel.

The LIC intelligence system consists of all host-country intelligence support and intelligence support provided by US forces channeled through the host structure. The national intelligence structure of the host country normally is established to direct information from all sources into a single channel. This channel leads to a central body whose responsibility is to produce a composite intelligence picture for the country as a whole. This central body is the host-country National Planning Coordination Center (NPCC). The NPCC is organized to direct and coordinate the collection, processing, production, and dissemination of intelligence. Intelligence operations at the subnational level are carried out at facilities called Area Coordination Centers (ACCs). The function and format of an ACC is similar to that of an NPCC. Supporting US MI activities develop close relations with the NPCC and ACCs counterparts. The interchange of personnel between all in-country ACC activities serves to educate those personnel and improve overall intelligence operations. ACCs have three missions. They are to—

- Provide integrated planning, coordination, and direction to all governmental efforts in their area of responsibility.
- Assure an immediate, coordinated response to operational requirements.
- Communicate with the people and invite their participation in programs designed to improve the economic, social, and political well-being and security of the area.

US Army MI efforts support the missions assigned to an assumed by the NPCC and ACCs by—

- Determining intelligence objectives.
- Integrating local intelligence programs with host-country national programs.
- Evaluating intelligence resources.
- Organizing and training new intelligence activities.
- Formulating new intelligence plans.
- Establishing priorities and allocating resources.
- Conducting an active liaison program.

In the event that US tactical forces are committed to a host country, the intelligence personnel of the tactical forces work with the combined intelligence elements already in place on a mutual support basis.

A description of LIC would not be complete without mention of urban terrorist and guerrilla activities. The terrorist strikes in urban as well as rural areas.

Urban terrain is analyzed using standard IPB methodologies. Urban terrain has both horizontal and vertical acreage that offers both the terrorist and the guerrilla tactical protection and vantage points. The terrain of an urban environment is different in terms of features, but the analytical methodologies are the same.

Man has created steel and concrete jungles which, in most cases, offer more opportunities for terrorist and guerrilla activities than natural jungles. The following describes the urban jungle:

- ☐ Stairwells and elevators.
- ☐ Roof tops.
- ☐ Vacant buildings and empty rooms in occupied buildings.
- ☐ Basements.
- ☐ Underground utilities.
- ☐ Sewer systems.
- ☐ Subways.
- ☐ Mass transit terminal systems.
- ☐ Other elements of key urban terrain which offer tactical advantages such as observation and fields of fire, concealment and cover, and structures and facilities which offer protection from NBC operations.

All traditional intelligence categories are used effectively during LIC situations. National policies and security constraints limit certain aspects of intelligence data which can be bilaterally shared without sanitization. Normally, there will be little, if any, terrain which will be completely denied to all US collection systems or activities. The host country will not, in normal circumstances, have sufficient hardware or knowledge to exploit the opportunities for intelligence collection which would be present in a LIC environment. The factors which inhibit effective collection operations are—

- ☐ Lack of OB data on the guerrilla insurgent force.
- ☐ Difficulties in differentiating insurgent military equipment from materiel indigenous to the area.

In a LIC, US MI personnel support the host country both in advice and assistance roles, and when required, as a part of military operations. The MI officers of various elements may have to coordinate requirements in innovative and nontraditional ways. Chains of command and political architecture of the host country are defined and used as the basis from which support channels are established.

The terrain and weather conditions of an anticipated LIC operational area are important considerations in terms of both the human factors and materiel maintenance. The conditions described in the following paragraphs also may apply to a LIC. Additional LIC information is contained in FM 100-20.

SPECIAL ENVIRONMENTS

The environments encountered in areas of US strategic concern are varied, and each exercises a unique influence on the conduct of military operations. This uniqueness is important in determining how Army doctrine is applied to individual challenges posed by each of these environments. Doctrine itself will not change.

This section describes the various special environments for which Army preparedness is maintained. It highlights the unique challenges of each environment and focuses on considerations for adapting core IEW doctrine to special operations in jungle, desert, mountain, winter, and urban terrain.

JUNGLES

The jungle regions of Asia, Africa, and the Western Hemisphere are potential battlefields. Jungles vary from tropical rain forests and secondary growth forests to swamps and tropical savannas. The dominant features of jungle areas are thick vegetations, high and constant temperatures, heavy rainfall, and humidity. Military operations in jungles are affected primarily by two factors—climate and vegetation. These factors combine to restrict movement, observation, fields of fire, communications, and battlefield intelligence collection operations. Both factors constrain MI units' operational and sustainment capabilities and demand extraordinary measures to minimize their effects.

Operational Considerations

Because of the nature of the jungle, tactical operations will be attached or placed in DS. Ground mobility restrictions require that IEW systems be lighter, manportable, and more rugged, and that they be fielded in greater densities. This also dictates an increased reliance on helicopters.

The climate, vegetation, and restricted LOS will significantly reduce the effectiveness of AM and FM communications. Jungle vegetation and humidity will absorb electromagnetic radiation by a factor of 10 to 25 percent. While landline is a logical alternative, maintenance and security considerations limit its use. Maximum use of hilltops and aerial relays is necessary to achieve effective C^2.

The lack of distinctive terrain features and poor map coverage of jungle areas limits location accuracy. Aerial observation and imagery collection are affected by canopy cover while vegetation limits the range of ground surveillance systems. HUMINT operations, particularly reconnaissance patrols, may be the most accurate, timely, and dependable sources of combat information and intelligence in jungle operations. Reliable information also may be obtained from friendly civilians living in the area.

Communication problems may arise as a result of terrain and the inability to reasonably protect landlines from destruction or monitoring. Jungle areas in which heavy rain, high humidity, and closely grouped tall trees dominate the terrain cause a communication phenomenon known as RF absorption. RF absorption affects higher frequencies more than lower frequencies, and vertically polarized antennas more than horizontally polarized antennas. FM equipment is affected more by absorption because of the higher operating frequencies and the use of vertically polarized antennas. However, AM systems operating at lower frequencies can employ horizontally polarized antennas. Currently authorized RATT equipment can be used in a voice or Morse mode by qualified personnel (operators holding additional skill identifier A4 (International Morse Code)).

Very detailed attention must be paid to noise, light, camouflage, and litter discipline, as well as preoperation reconnaissance and artillery preparations. Effective small unit OPSEC is absolutely vital in the jungle.

Environmental constraints reduce the effectiveness of EW in the jungle. Vegetation limits the effective range of jamming and ESM collection. This may be offset in part by the use of aerial resources.

Sustainment Considerations

High incidence of rust, corrosion, and fungus caused by jungle moisture and humidity increases the necessity for daily maintenance on equipment—especially at the operator level. This is especially true for electronic systems and encryption equipment which are subject to very high failure rates in jungle environments. Continuous operation of such systems generates heat which combats moisture, corrosion, rust, and fungus decreasing the mean time between failures but hastening system wearout.

Increased reliance on helicopter mobility, especially for supplies, demands command attention be placed on supply discipline to reduce resupply rates and ensure helicopter availability for operational missions.

Troop health hazards in a jungle environment are a serious threat to foxhole strength. Individual sanitation, protection, and acclimatization against gastrointestinal disease and fungus infections are vital.

DESERTS

Many desert areas of the world are potentially vital to the national interests of the United States and demand Army preparedness. Deserts may be semiarid or arid so the availability of water is a prime factor in planning and conducting desert operations. They are characterized by the extremes of cold and heat, unequaled visibility and blinding sandstorms, drought and sudden rains, water shortages and flash floods, or excellent trafficability and interspersed obstacles. Military operations in the desert are characterized by rapid movement of large units, good observation and long fields of fire, mandatory use of deception, and lack of what has traditionally been considered key terrain.

Operational Considerations

The vastness of the desert necessitates wide dispersal of units and SIGINT and IMINT systems. System density is considered when task organizing the force. Additional assets are highly desirable, but may not be available. The desert environment also will necessitate centralized operations at brigade and division level. This requires more DS and general support reinforcing missions than in Central Europe. The mobility factor of the desert requires more tracked and fewer wheeled vehicles for IEW systems.

The desert climate causes some degradation in AM and FM radio communications due to thermal heating and dead spots. Communications during hours of darkness are excellent. During daylight, heat, dryness, and soil mineral content can cause 20 to 30 percent loss in radio communications. Strong temperature inversions and moisture layers found in many desert regions can have severe consequences on electromagnetic wave propagation of all types. In addition, frequency crowding will limit radio capabilities. RATT will suffer frequent downtime from sand and dust if unprotected. Communication links are established during the more severe daylight conditions at high power settings. During more favorable conditions, low power settings are used when possible. Wire should be employed to enhance communications security.

Within the limitations cited, the desert environment is well suited for the operation of IEW systems. Operator maintenance of equipment is required on a continuous basis to keep sand and dust from seeping into critical items. IMINT systems are subject to heat wave distortion and dust storms which limit their overall usefulness. Nevertheless, these systems provide extremely valuable intelligence in the desert. However, long-range reconnaissance patrols, strategic offensive forces, and irregular force operations produce HUMINT useful for planning and data base confirmation. S&T intelligence identifies the technical vulnerabilities of critical systems and critical resources for denial. It also provides a source of technical advice and assistance to tactical cover and deception (TC&D) operations. The importance of terrain intelligence is increased in the desert because of map inaccuracies and the relative absence of traditionally encountered key terrain. Small discriminations in terrain are identified, recorded, and disseminated. Weather intelligence value is consistent with standard doctrine.

OPSEC increases in importance due to the long range of IMINT and SIGINT systems in the desert. COMSEC and camouflage, supported by deception and intelligence, are vital in preserving the security of any force. The enemy intelligence system must be deceived or no advantage on the battlefield will be possible.

Like OPSEC, the value of EW on the desert battlefield has increased importance. The expansiveness of the desert precludes using terrain masking to avoid jamming. EW can freeze the battle for destruction by fire and maneuver, and plays a significant role in air defense and CAS suppression.

Sustainment Considerations

The dust, sand, and heat of the desert place heavy requirements on preventative maintenance checks and services and unit maintenance. Excessive dust and sand cause contamination of POL. Sand gets into internal mechanical parts through air intakes and increases wear. Excessive heat causes overheating and burnouts in vehicle electrical systems as well as in all types of power generation equipment. In addition, the gravelly consistency of desert soil extracts a heavy price on tires, tracks, and vehicle suspension systems. Command supervision and active involvement in maintenance is an important element of success in the desert.

Units operating in the desert use a higher volume of repair parts than units in Central Europe. Unit prescribed load lists (PLL) and authorized stockage lists (ASL) should be increased by as much as 40 percent for such items as tires; fan belts; filters for automotive, generator, and C-E equipment; tow chains; clutch plates; shocks; and track pins.

Acclimatization training for the desert is a must to ensure soldier sustainment. Leaders must insist that total environmental training is conducted before arrival in the desert. Soldier sanitation and hygiene are practiced. The untrained soldier is susceptible to dehydration, heat stroke, heat exhaustion, snake bite, and numerous physiological and psychological disorders which come from improper desert operating practices.

Additional information on desert operations is contained in FM 90-3.

MOUNTAINS

Mountainous terrain exists throughout the world from the northern regions to the tropics and significantly impacts on military operations. Mountain operations are characterized by—

- Reduced ranges for direct fire weapons.
- Increased importance of indirect fire.
- Mobility canalized along valley floors.
- Decentralized combat.
- Increased collection operations from heights dominating LOCs.
- Reduced C^2 capabilities.

Operational Considerations

Because of canalization, greater reliance on the helicopter for troop movement, resupply, and medical evacuation is required. Use of helicopters can be limited by density altitude, clouds, fog cover, and icing, and can necessitate pilot oxygen requirements at higher altitudes. This requires that IEW systems be rugged, light, and manpacked to exploit the surveillance advantages offered by the higher elevations. Once within the mountain complex, IEW systems must be manpacked because most movement is by foot. Because of the compartmented nature of the mountain terrain, combat operations tend to be piecemeal and decentralized requiring more DS and attachment. This decentralization also demands a higher density of IEW systems to ensure sufficient coverage.

The rugged, irregular terrain degrades normal AM and FM radio effectiveness as well as associated C^2. Heavy reliance on relays and retransmission stations is required. The use of wire is limited by the difficulty of maintenance.

HUMINT is a very valuable source of intelligence in the mountain environment. The heights offer numerous sites for OPs which may nullify the effect of terrain masking. OPs are supplemented with reconnaissance patrols. In the valley areas, population centers may provide a HUMINT collection and interrogation potential, especially for terrain intelligence information. The majority of IMINT and SIGINT will be provided by aerial systems.

Weather intelligence will be of prime importance because of the highly erratic weather patterns associated with the mountains. Cloud cover, fog, rain, winds, and normal seasonal variations have a significant impact on military operations.

A defending enemy force will enjoy a distinct advantage in terms of terrain and the ability to deceive. For an attacker, OPSEC will be of major importance, as will be the ability to deceive the enemy.

The irregular terrain patterns, abundant dead space, and degraded C^2 will render EW less effective in the mountains than in other types of terrain.

Sustainment Considerations

Equipment used in a mountainous environment must be rugged, light, and manportable. Cold weather in the higher elevations or during seasonal variations will affect equipment in the same manner as in winter operations.

Transportation limitations will require greater use of field expedients than in other types of operations. Because of the rugged nature of the terrain, greater consumption of class IX repair parts will occur and demand a 20-percent overage in PLL and ASL for such items as tires, transmissions, clutch plates, filters, brake shoes, tracks, track pads, and fuel pumps.

The key to sustaining soldiers in the mountains, as in other special environments, is training. Mountain combat can

affect a soldier's mental alertness, accentuate fears of heights and closeness, and cause dehydration and sickness.

Additional information on mountain operations is contained in FM 90-6.

WINTER CONDITIONS

The effects of winter conditions have a significant impact on military operations. Winter is characterized by long nights, extreme cold, and deep snow. Its effect on military operations can be degradation of weapons performance due to brittleness, ice fog over optic sights, and ice loading on antennas and intake filters. Winter conditions increase the time required to perform even simple tasks, and adversely impact on soldier health and morale.

Operational Considerations

Due to the extensive snow covering of the terrain, mobility can be canalized along major LOCs, unless the land surface is frozen making cross-country mobility possible. The use of helicopters for transportation, resupply, and reconnaissance tends to offset this mobility constraint. IEW systems should be either manpacked for movement by helicopter or track-mounted for surface movement. Like other extreme environments, winter operations are decentralized, necessitating a larger than normal use of DS missions and attachment for MI elements. MI units operating in a winter environment should also be afforded a higher density of IEW systems than normal due to the severe terrain and climate conditions.

HUMINT and IMINT are two important sources of intelligence in winter operations. The extensive reliance on reconnaissance and patrolling, employment of special operating and irregular forces, and the use of indigenous scouts all serve to increase the value of HUMINT. IMINT systems, especially photo capabilities, are a valuable source of intelligence with respect to contrast, long shadows, and track activities. SIGINT systems are potentially very valuable, given the extensive reliance on radio communications; however, they are so sensitive to extreme cold that their availability will be limited. Aerial platforms are subject to icing conditions which limit reliability and usefulness. Terrain and weather intelligence continues to be critical.

Camouflage is very difficult to achieve effectively in a winter environment. However, concealment is easier to attain making maximum use of dispersion, vegetation, darkness, fog, and falling snow. Bivouac areas, motor parks, and large numbers of warming shelters are difficult to conceal. COMSEC also requires added emphasis because of the extensive use of radio.

The increased role of radio communications, the essential part played by all types of aviation support, and the importance of air defense, all combine to produce a lucrative environment for EW. Electronic deception is accentuated in winter operations.

Sustainment Considerations

The major impact of winter operations on equipment is caused by cold and snow. Extremely low temperatures cause metal parts of weapons to become brittle resulting in a high breakage factor for internal parts. Vehicle engines and generators require frequent starting and the frequent starts cause condensation in the internal parts of the engine which later freezes. The intake filters of carburetors and C-E equipment are particularly susceptible to icing. Condensation covers on microphones and telephone handsets ice frequently if not protected. Blowing snow will also jam air intake valves. Pneumatic antenna masts and ADP equipment freeze because of condensation and freezing temperatures. Batteries provide only a fraction of their normal power when they are cold. RATT equipment is very susceptible to malfunction in these circumstances.

Units preparing for winter operations require a larger than normal PLL and ASL. Each unit will need larger class III allocations because of frequent engine starting. Higher PLL usage factors will be experienced for filters, batteries, spark plugs, hydraulic hoses, and all types of seals. Less viscous lubricants are required.

In winter operations the human element is all important and demands concerned

leadership and thorough training. Particular attention must be given to minimizing the effects of vision whiteouts with the attendant loss of perception which affects driving and flying. High windchill factors and the potential problems of frostbite and immersion foot are additional considerations. Cold weather training experience is absolutely essential prior to deployment to the operational area.

Additional information on cold weather operations is contained in FMs 31-70 and 31-71.

URBAN TERRAIN

Commanders have always recognized the importance of urban centers as strategic objectives but the direct seizure of cities and towns has always been difficult. Committing forces to urban areas should not be undertaken unless the attacker or defender can realize significant advantages. The Army must be prepared to exploit the advantages of urban terrain. Military operations in urban terrain are characterized by shorter engagement ranges, structural obstructions to observation, extreme canalization, obstructed communications, and the addition of a new vertical dimension provided by sewer systems and buildings. There are frequent limitations posed by rubble obstacles, control of civilian populations, and the greatly reduced effectiveness of reconnaissance and surveillance systems. These factors constrain MI unit operational and sustainment capabilities and demand imaginative and innovative solutions to minimize their effect.

Operational Considerations

The fragmented and compartmented nature of urban combat necessitates decentralization of operations. MI elements normally are placed in DS of, or attached to, maneuver units assigned combat missions in urban areas. Vehicle-mounted SIGINT systems are less useful than manpacked equipment because of restricted LOS.

The urban environment restricts or limits the effectiveness of AM and FM communications for C^2. More use should be made of wire and operational civilian telephone systems. In addition, FM frequency crowding may be experienced, and the best use of FM will be in conjunction with tall buildings or towers which provide unobstructed LOS.

The IPB efforts which precede operations in urban areas should include the collection and analysis of city plans. City plans include buildings and structures, sewer and subway networks, and the specific location of key targets for destruction or retention. HUMINT is effective in collecting information from local inhabitants, gathering terrain information, and identifying residual pockets of enemy resistance. CI personnel seek to neutralize the remaining enemy intelligence collection systems, and take advantage of the support of local police and civil administration. OPs on high buildings eliminate dead space and provide complete surveillance coverage. Reconnaissance patrols and aerial observers also are excellent collection means. Terrain intelligence supplements existing map coverage with locally acquired data. S&T intelligence will provide considerable insight into enemy sustainment capabilities. S&T intelligence personnel of the EAC MI brigade will examine enemy training areas, depots, and discarded equipment and exploit factories and laboratories. IMINT and SIGINT collection will be reduced primarily due to LOS obstructions caused by structures. SIGINT collectors use towers and tall buildings in the urban area to cover terrain outside the built-up area and between villages. Aerial imagery can enhance terrain intelligence. Any enemy use of civilian telephone systems and landlines can be exploited for SIGINT.

Defender advantages of concealment and cover; protected, elevated platforms for IMINT and SIGINT systems covering approaches to the urban areas; and the ability to hide key installations without risk of detection all place a premium on good OPSEC. The urban environment limits the use of EW. However, airborne EW systems may be useful in disrupting the enemy command and control links from higher echelons.

Sustainment Considerations

There are no unique sustainment considerations for MI equipment, supplies, and soldiers in the urban environment.

Additional information on operations on urbanized terrain is contained in FM 90-10.

CHAPTER 13

Joint And Combined Operations

Any future conflict of any significance will undoubtedly involve major US land, air, and naval forces operating in concert—joint operations. It is also very likely that US joint operations will be conducted as part of a larger effort involving allied forces—combined operations. The advent of World War II marked the beginning of an era in which joint and combined military forces have increasingly been used as the primary means of waging war. This trend shows no sign of reversing itself. This chapter describes the organizations, responsibilities, principles, considerations, and processes that make up the IEW operations so critical to joint and combined military forces.

JOINT OPERATIONS

The joint IEW system includes the IEW staffs, agencies, and resources in the joint and component commands and at ECB. The system supports the unified, specified, and component commanders during peace, crisis, and war. During peace, IEW supports contingency planning and training. It plans for the full spectrum of military operations including such sub-hostility operations as evacuation of US citizens, disaster relief, humanitarian assistance, and peacekeeping. During crisis situations, collection and analysis activities are increased to satisfy the force commander's PIR. During war, the system supports battle coordination at joint and tactical levels. It also supports rear operations.

The missions of IEW agencies and units supporting a joint command include—

- Collecting, producing, and disseminating intelligence necessary to plan and execute assigned missions.
- Providing IEW support to subordinate elements of the joint force.
- Discharging intelligence missions and functions assigned by higher authority.
- Planning, coordinating, and integrating EW operations.
- Directing CI operations.

PRINCIPLES

The same principles that guide IEW operations at lower tactical levels are appropriate at joint command level. However, the nature of joint IEW organizations, missions, and operations dictates that additional principles be followed to ensure a coordinated and effective effort. The following principles will not ensure success or even cover all contingencies; however, they are vital ingredients of all joint IEW operations:

- Develop a single intelligence product.
- Integrate joint IEW operations into a total IEW system.
- Centralize IEW support functions.
- Conduct peacetime transition training.
- Employ ADP support for IEW operations.

A single intelligence product is developed rather than separate products addressing the air, land, and naval force aspects. Similarly, EW and CI are integrated to achieve the most effective use of resources. Although each component has unique IEW requirements, they are integrated at the joint level. This principle is achieved through joint staff structures and IEW fusion centers composed of personnel from all components of a joint force.

The IEW effort is coordinated throughout the joint command and with US and allied national intelligence operations. Joint IEW systems must be an integral part of the

IEW architecture that extends from the tactical to the national level. Interoperability and mutual support between all components and echelons within a command are essential. Duplication of effort must be avoided.

IEW support functions are centralized when it is expedient and efficient. Responsibilities should be assigned to the component best able to perform the function. If it becomes obvious that no component within the joint force can properly perform the specific function, the commander of the joint force may establish intelligence agencies responsible to the joint staff intelligence division, JIC.

Peacetime planning, operations, and training facilitate a rapid transition to war. Missions, organizational structures, C^2 relationships, operating procedures, and coordination channels must be designed to meet wartime requirements and to be modified for peace. IEW data bases are maintained and updated continually and include inputs from all component and national systems. Peacetime training and operations stress the development of procedures for employment in war.

Automated assistance is required to manage joint IEW data bases and to effectively process a heavy flow of IEW data. Digital links between critical IEW fusion centers will enhance interoperability and speed the flow of information.

STAFF

A joint staff is established at the joint command level to coordinate air, land, and sea operations. A joint J2 and J3 staff structure is vital to effective coordination of the IEW effort. A joint staff structure can better satisfy the needs of both the joint and component commanders.

J2 and J3 staffs coordinate and provide the commanders operational guidance. The joint commander has the authority to direct component commands not under the operational control of an allied command to collect specific types of information or perform specific IEW functions. The intelligence division (J2) provides operational direction for intelligence and CI operations while the operation division (J3) does the same for OPSEC and EW.

Joint IEW staff organization should reflect consideration of a number of factors. The joint staff must not only consider the IEW needs of the parent command and its subordinates, but also those of higher and adjacent headquarters. It should provide the degree of centralized control that will best benefit all elements of the command. Where distance or operating conditions would cause delay in the production or dissemination of intelligence, forward staff agencies may be established.

The joint intelligence staff coordinates the intelligence effort. It integrates intelligence received from the component IEW systems with that provided by the joint, national, and allied agencies to produce an all-source product to satisfy the needs of the joint commander.

There are two basic types of joint intelligence staffs. The first is a relatively large, self-supporting staff. It includes all staff elements required for planning, policy formulation, coordination, and processing and dissemination. A regional variation of a large staff is shown on the following page.

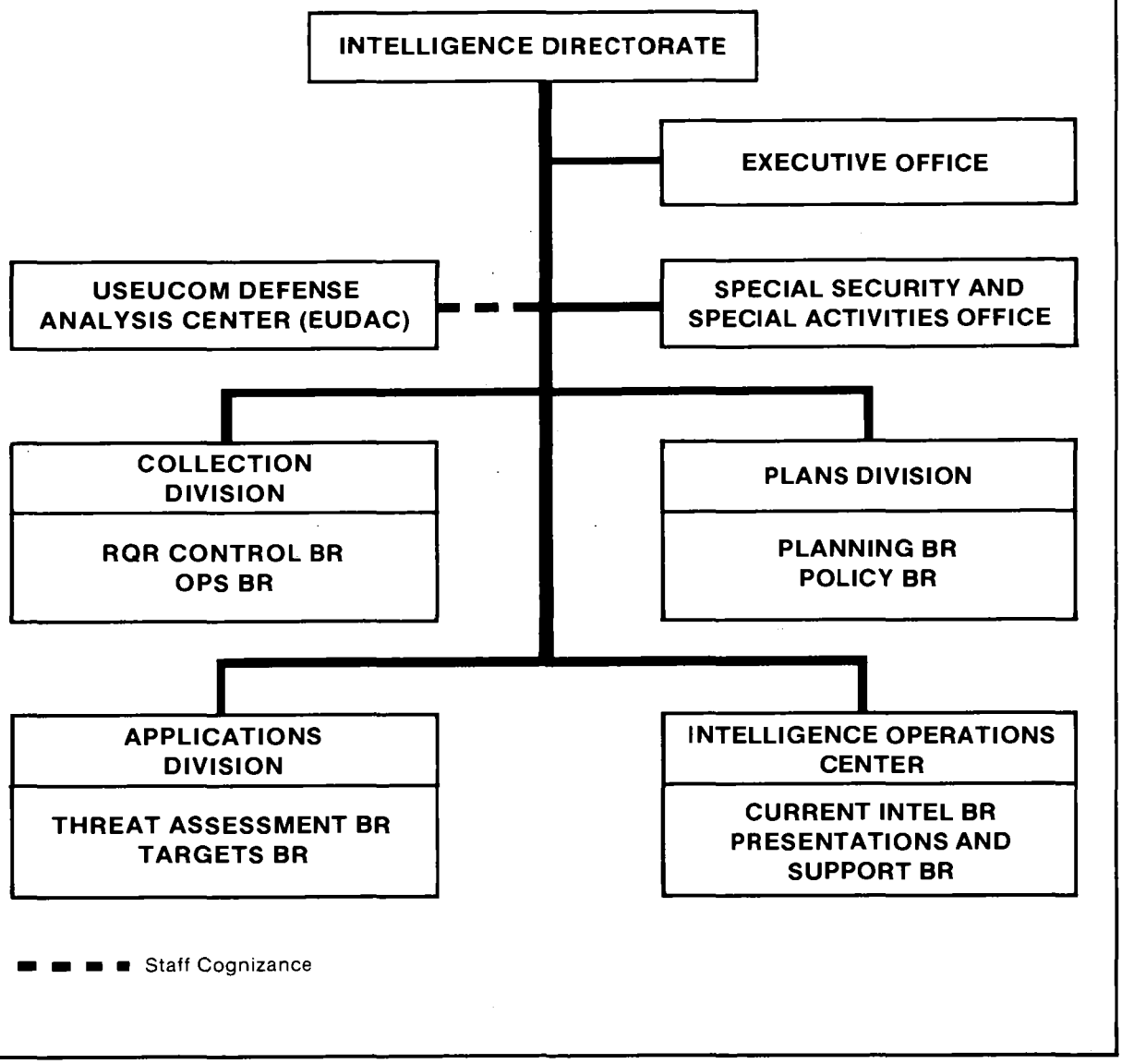
The second is small and is more dependent on subordinate commands for support. The smaller staff confines itself primarily to policy formulation, planning, and coordination. It relies on the IEW organizations of subordinate component commands for collection, production, and dissemination of intelligence. To facilitate intelligence operations, the joint force commander may form a JIC out of the joint intelligence staff and supporting elements from component commands.

Joint Intelligence Center

The JIC integrates the intelligence efforts of the component commands to provide intelligence essential to the joint force commander and staff and to supplement that available to subordinate commands. The JIC—

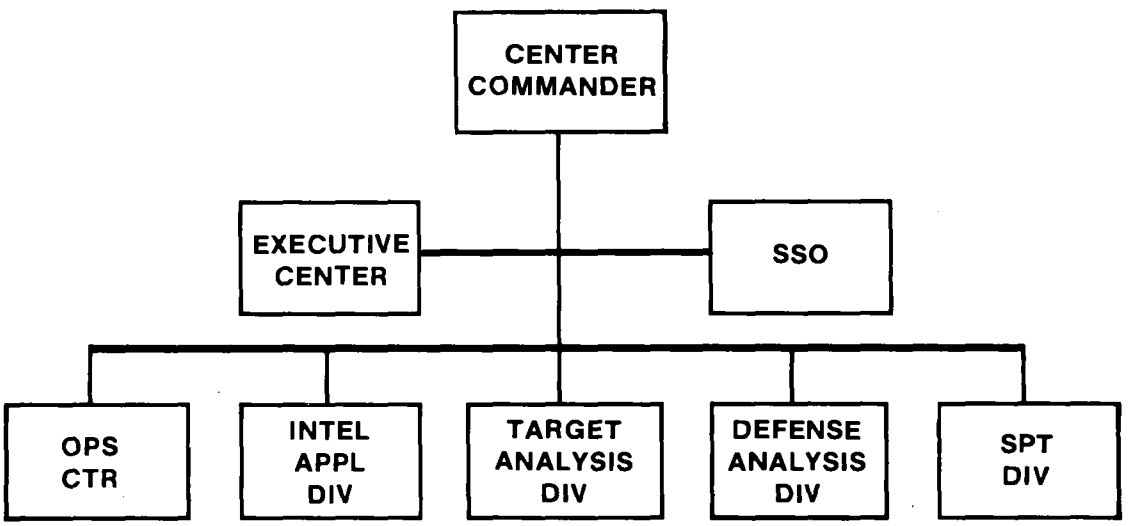
- Coordinates joint intelligence collection operations.
- Provides the joint, component, and tactical commanders with a coordinated view of the battlefield.

US EUROPEAN COMMAND J2 ORGANIZATIONAL CHART



- Tasks joint and component command collection assets through appropriate tasking channels.
- Provides centralized control of national assets placed OPCON to the joint force.
- Provides technical advice and support to subordinate command IEW staffs and units.
- Produces integrated all-source intelligence.
- Obtains intelligence support from national intelligence agencies and provides intelligence developed within the joint command to national agencies.
- Disseminates intelligence and targeting information.

JOINT INTELLIGENCE CENTER ORGANIZATION CHART



- Provides IEW support to US Military Assistance Advisory Groups (MAAG).

A type JIC is illustrated above.

In combined operations, the JIC may locate US intelligence support elements (ISE) at combined and allied commands to facilitate the mutual exchange of IEW information. The ISE interoperates directly with the JIC. It identifies the supported command's IEW requirements and establishes priorities. It passes the IEW requirements of the joint command to the combined or allied IEW staff, and assists in the interpretation of IEW data. The ISE provides communications equipment compatible with US equipment if required.

A special interdependency exists between a joint force and national-level intelligence agencies. Joint forces are dependent on strategic, technical, and current intelligence developed by national agencies. National agencies rely on joint force information and intelligence, including that developed by component commands. Joint forces represent a significant part of DOD collection capabilities.

Joint force intelligence agencies, including component agencies, are linked directly with national intelligence agencies for tactical exploitation of national capabilities

(TENCAP) and national exploitation of tactical capabilities (NETCAP). Tactical units request information from or forward information to national agencies directly or through joint or component command intelligence channels. National intelligence agencies may, in turn, forward information directly to subordinate tactical commands (such as an Army corps) at the same time it is forwarded to the higher command.

Joint EW Staff

The joint commander's EW staff (JCEWS) reinforces the joint commander and the J3 in coordinating EW operations throughout the command. It provides each component the flexibility to satisfy their EW requirements consistent with the need to avoid mutual interference with friendly systems. The JCEWS facilitates cross-service EW support and the mutual exchange of EW technical data. (See the following illustration.)

The JCEWS advises and assists the J3 in carrying out EW responsibilities. It—

- Prepares EW estimates and annexes to joint OPLANs and OPORDs.
- Coordinates EW operations.
- Evaluates the impact of friendly and enemy EW activities on joint force operations.
- Monitors the status of available EW resources.
- Monitors the use of aerial EW assets and coordinates airspace required by aerial EW operations.
- Acts as the joint focal point for preplanning and integrating EW operations.
- Monitors EW request nets to expedite actions and resolve conflicts.
- Establishes priorities for EW support based on the joint commander's concept of the operation.
- Assists in emission control (EMCON) planning.
- Assists in deception planning.
- Coordinates with the J2 for SIGINT and ESM data required for planning and coordinating EW operations.
- Coordinates with the C-E officer (J6) to ensure ECM do not interfere with friendly C^2 and communications.

Joint use of EW is coordinated and tasked at the component command level when possible. EW staffs within component command operations centers establish and maintain close and continuous liaison with their counterparts in the other components. When EW support cannot be coordinated or resolved at the component command level, assistance is requested from the JCEWS. However, due to communication delays, such support requires considerable lead time.

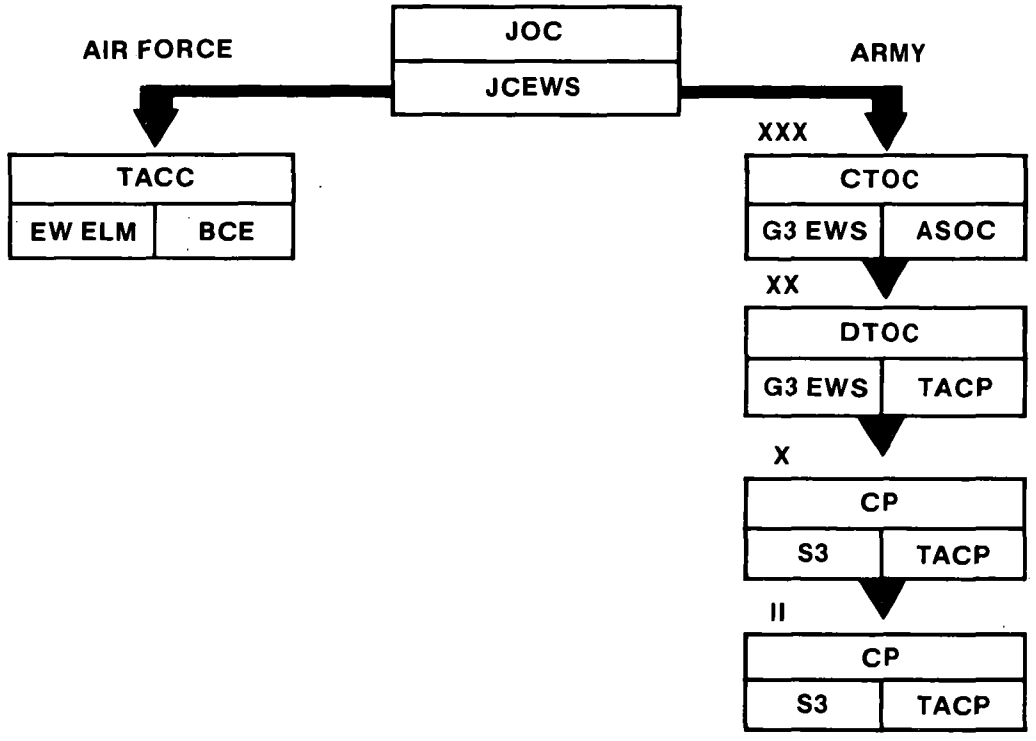
The corps G3 coordinates joint EW support of the land battle. This is done through the air support operations center (ASOC) and the battle coordination element (BCE).

The Army provides a BCE at the Air Force tactical air control center (TACC) to ensure Army operations and requirements are coordinated with the Air Force. The BCE monitors and analyzes the land battle for the TACC, and provides the interface for exchanging intelligence and operational data between the CTOC and TACC. Based on the battle plan and the commander's guidance, it establishes priorities for corps requests for Air Force EW support.

The Air Force TACC EW element coordinates joint EW activity in support of air operations. The Air Force provides an element at each level of command of the Army force to coordinate air operations. An ASOC is located at each corps TOC to interface directly with the corps staff. Tactical air control parties (TACP) are located with divisions, brigades, and maneuver battalions to coordinate air operations at these levels.

The immediate control, direction, and supervision of intelligence, CI, and EW assets are usually handled by component commanders. In wartime, however, geographic locations, communications means, and economy of resources may dictate that the joint staff exercise direct control and supervision of some component IEW assets.

JOINT ELECTRONIC WARFARE ORGANIZATION



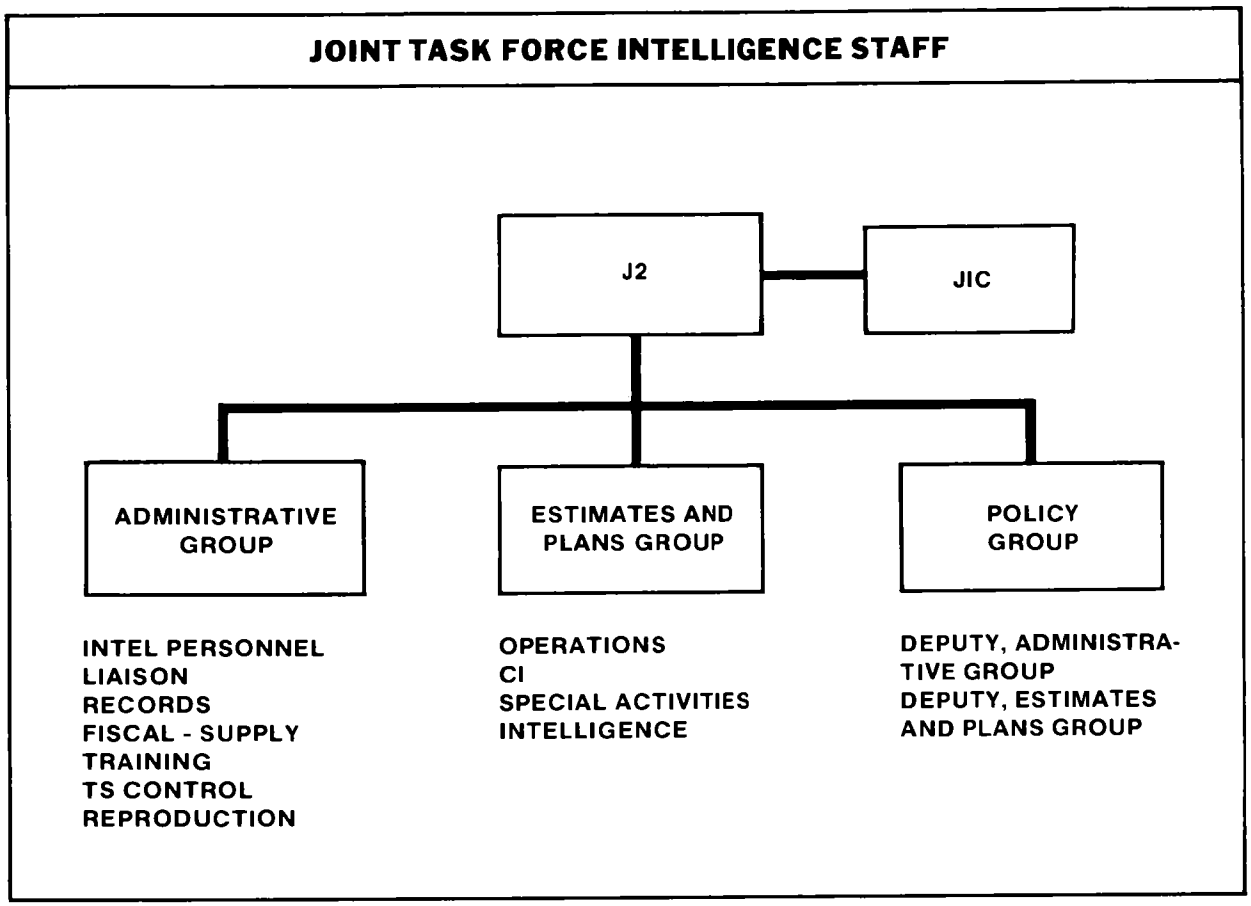
In any event, the IEW effort must respond to the requirements of the joint command as well as the component commands. These requirements are set forth in intelligence, CI, and EW plans prepared at each joint echelon and disseminated throughout the command.

JOINT TASK FORCE IEW STRUCTURE

IEW needs at the JTF level are normally less than those of higher level joint commands. The JTF mission is limited in scope and duration requiring mostly tactical intelligence. However, EW needs may be very significant, and the JTF becomes intimately involved in the specific planning and coordination of EW operations.

Time is normally a limiting factor in planning and conducting IEW operations in a JTF. Forces may not be assigned to the JTF early enough to permit reconnaissance and development of its initial data base. It relies on the superior joint command for much of its data requirements and considerable support during the operation. It also relies on the capabilities of subordinate component IEW elements.

The size and type of IEW organizations for a JTF will vary greatly. A typical JTF intelligence staff organization is illustrated in the following chart.



CONTINGENCY OPERATIONS

Contingency operations involve the deployment and use of US forces, usually a joint force, by the direction of the national command authority (NCA) in support of national policy. The size of a contingency force, its mission, and the area of its employment can vary widely. Plans may already exist for these situations, or unforeseen conditions may preclude detailed prior planning.

The IEW system is organized to provide integrated IEW support for contingencies at all levels. Units are tailored to support the needs of unified, specified, and combined commands, other EAC commands, and CONUS-based organizations with a contingency mission.

To ensure worldwide coverage of areas of US interest and to support both forward-deployed and contingency forces, IEW organizations are assigned region-oriented missions worldwide. In areas where a major conflict is possible, IEW organizations should be in place and operating in case of a crisis or war.

During peacetime, IEW operations are focused on satisfying contingency planning requirements and developing the capability to satisfy wartime requirements. Peacetime contingency planning requires current, all-source intelligence. Intelligence operations must be initiated early in order to satisfy this requirement. The IEW system must develop and coordinate sources for collecting required information and build data bases to store, retrieve, and manipulate this information to satisfy planning requirements.

Data base development and source control may be performed by either a designated regional IEW unit which has been assigned the mission to support contingency operations in a specific area, or from

a designated IEW unit in the CONUS base. An IEW unit supporting a contingency force will develop its data base through directed collection using its own assets and by exploiting the data bases of national-level agencies.

Updating the data base and satisfying intelligence gaps requires active coordination between the contingency force IEW system and the national intelligence system. National intelligence assets with deployed IEW units play a key role in fulfilling the contingency commander's intelligence requirements. After deployment, these systems continue to augment contingency force collection assets in the operational area.

During peacetime, IEW operations cover the areas where the contingency force is most likely to be employed. During crisis situations the focus is shifted to a specific objective area, and the contingency force commander is provided only that information that is pertinent to operations in that area. Continuous maintenance of data bases during peacetime permits rapid identification of intelligence gaps which become immediate collection requirements during a crisis.

Upon execution of a contingency plan, the IEW system provides continuous support during the predeployment, deployment, and operational phases.

Predeployment actions by the IEW system in support of a contingency force commander include—

- ☐ Refining IEW requirements.
- ☐ Increasing collection operations to satisfy the contingency force commander's PIR.
- ☐ Initiating requests for additional intelligence collection from national systems.
- ☐ Increasing the frequency of IEW data base updates on contingency areas of operations.
- ☐ Increasing the frequency and timeliness of information provided to subordinate elements of the contingency force.

As deployment commences, an ISE deploys with the contingency force command group. The ISE serves as the interface between the organic IEW capabilities of the contingency force and national intelligence systems. If additional IEW units are needed to support the operation, they deploy to the contingency area of operations as soon as the situation permits. A tailored JIC or an EACIC will normally accompany a reduced headquarters element. As the theater matures, additional IEW capabilities will be deployed.

COMBINED OPERATIONS

Many contingencies involve US joint or Army forces operating as a part of a combined allied force. In Europe as part of NATO and in Korea as a part of the ROK-US Combined Forces Command, US forces operate under principles and procedures which have been developed, practiced, and standardized in peacetime. In other potential combat areas where combined forces may be established, agreements on principles and procedures are either nonexistent or only partially developed. These operations present the most demanding circumstances for commanders and intelligence and operations staffs. Procedures to integrate US and allied operations will have to be developed after the outbreak of hostilities.

Combined operations with even our closest allies present some problems that might hinder the accomplishment of common objectives. Each nation has unique capabilities, needs, and methods of operation. Each has its own economic, political, and sociological system. These differences may be compounded by different languages and customs. IEW operations must respond to the unique environment that may exist within each theater.

A multinational IEW system at combined echelons is essential to achieving the full cooperation and participation of allied resources in coordinated IEW operations. The system must include representation from each national force within the command. Combined IEW staffs and support

organizations provide a means for the mutual exchange of IEW requirements and data and coordination of collection requirements. Combined staffs and intelligence centers enhance cooperation, coordination, and interoperability between all elements of the combined force. Centralized analysis at the combined level provides a coordinated perception of the battlefield and promotes mutual understanding.

PRINCIPLES

Combined operations are based on the same principles by which joint operations are conducted. However, the inclusion of forces from two or more countries in the same force requires that other factors be considered to achieve an effective and coordinated effort. The diverse nature of allied forces and their tactical doctrine, national prerogatives, and other differences create obstacles to a unified IEW effort. The following considerations provide a guide to overcoming these obstacles and raising the level of cooperation and coordination among allied forces participating in combined operations:

- ☐ Develop a combined IEW system.
- ☐ Establish channels for the flow of IEW data.
- ☐ Establish standard procedures for IEW operations.
- ☐ Develop a secure, reliable communications capability.
- ☐ Ensure a linguist capability.
- ☐ Establish liaison between allied IEW units.
- ☐ Establish a common data base including formats.
- ☐ Ensure interoperability of equipment.

The combined system must be based on multinational all-source inputs, analysis, and dissemination to support the combined and subordinate national commands. It must provide access to intelligence developed by allied national and theater resources. It must have tasking authority over all IEW elements within the combined force. It must provide for effective coordination of the IEW effort and a free and timely exchange of IEW requirements and intelligence data.

Channels for exchanging IEW requirements, combat information, and intelligence must be established for peace and war. Security requirements, traffic volume, and command and control relationships may require that different tasking and reporting channels be used during peace, crisis, and war. However, the wartime flow must be defined in advance. It must provide for a rapid flow of information laterally and vertically and an efficient transition from peace to war.

Standard tasking, reporting, and dissemination policies, procedures, and formats enhance understanding and interpretation of requirements, information, and intelligence. Standard procedures that are practiced in peace will enhance a quick transition to war. Agreements between allies regarding the exchange of IEW data, such as third party release of information, should be negotiated prior to hostilities. Standardization agreements (STANAG) and quadripartite standardization agreements (QSTAG) are examples of standardized procedures agreed on by the allies in peacetime to enhance wartime operational efficiency.

Dedicated, secure communications systems are required to ensure timely tasking, coordination, and dissemination. Interoperability of communications equipment must be assured to permit operations in both US and allied IEW nets. If equipment is not compatible, a system of equipment exchange may be established.

US intelligence personnel must be capable of communicating in the language of the allied forces with which they will operate. Interpreters and translators must be trained on common IEW and technical terminology. In addition to linguists, all operational US MI personnel should receive training in basic communication in the allied languages. Key word lists, phrases, reporting formats, and terminology used in IEW operations and printed in multiple languages will help facilitate the communications process.

Liaison is vital in a multinational structure. Liaison teams ensure a free exchange

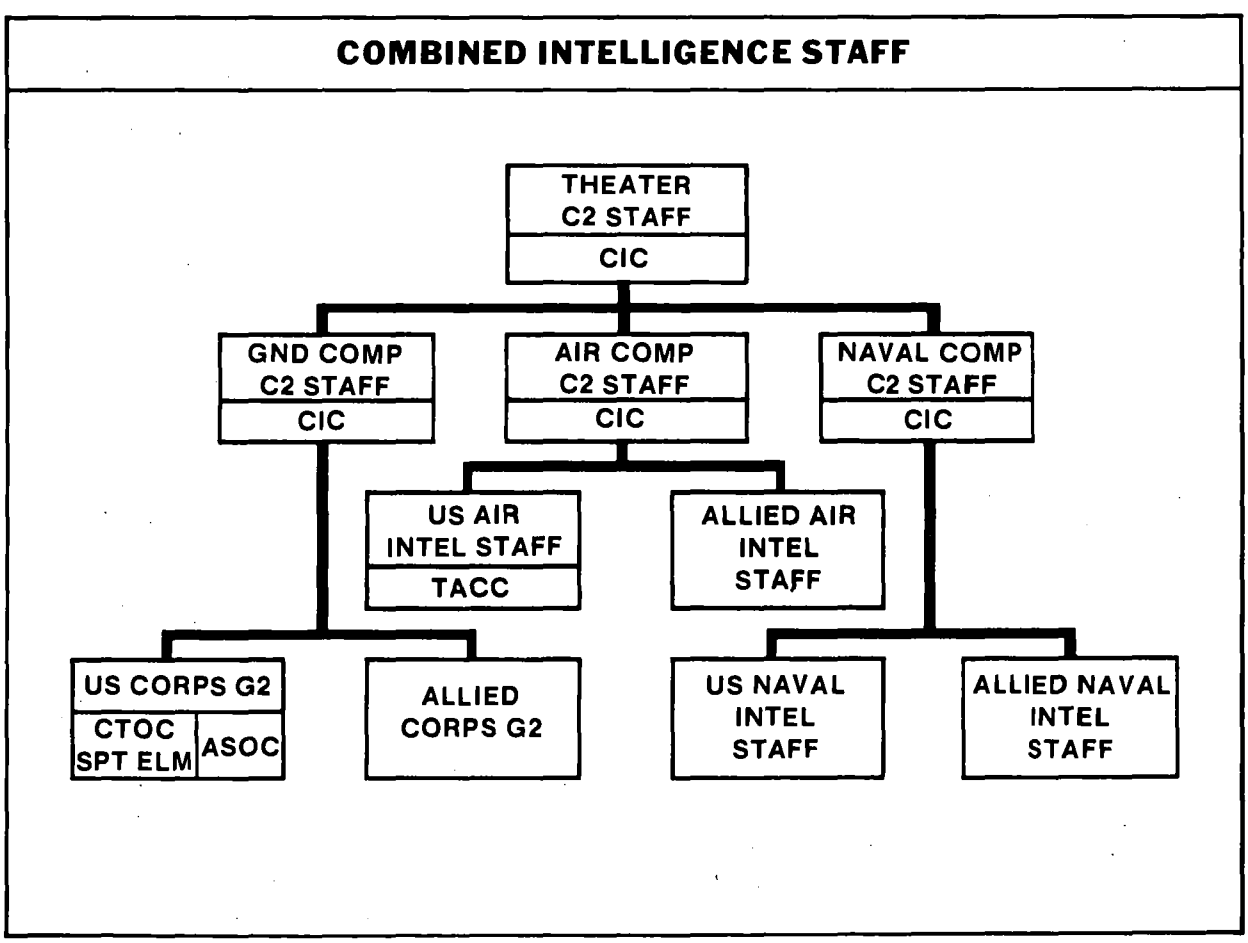
of IEW information and support. They prevent or reduce misunderstandings over procedures and terminology. Bilingual liaison teams must be knowledgeable of the doctrine, organization, procedures, and equipment of both US and the allied forces.

A data base developed through a combined effort during peace will enhance a quick and efficient transition to wartime intelligence operations. The data base should be composed of all-source data provided by all allied intelligence systems in accordance with national restrictions on the exchange of information. Combined analysis based on IPB techniques will provide a common perspective of the threat and enhance a coordinated intelligence operation in case of war.

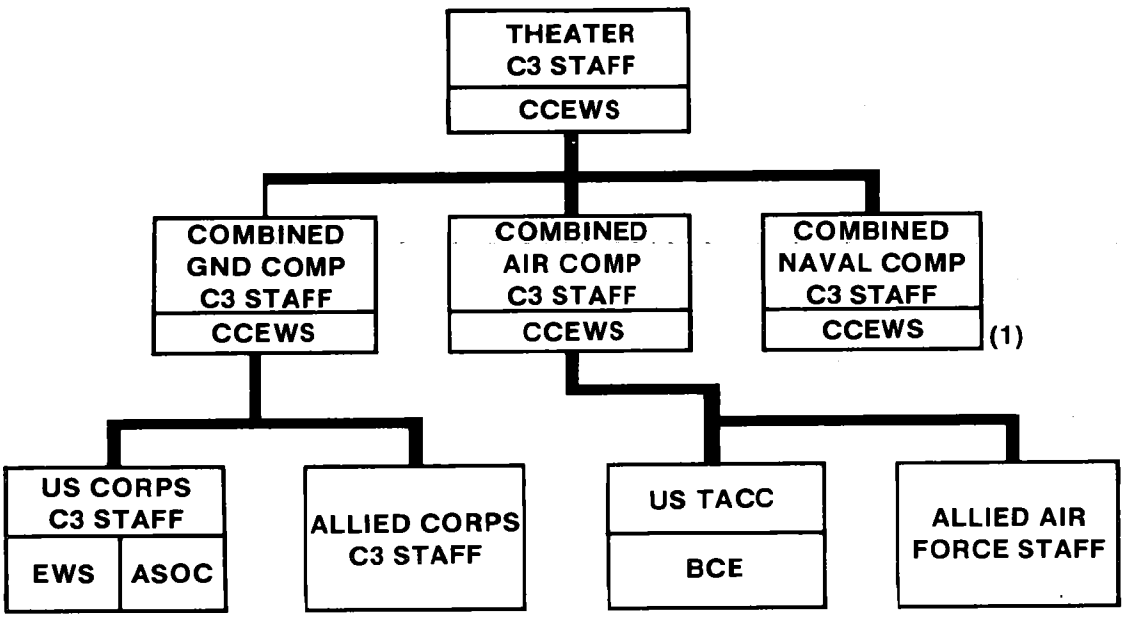
STRUCTURE

Due to the diverse nature of combined forces and respective theaters of operation, the development of combined IEW systems is dictated by the nature of the supported force and theater. Each combined force or theater of operations is unique. Thus, the IEW system that supports these forces must be tailored to each environment. The following charts illustrate types of combined force IEW systems.

The combined intelligence system must provide for the input of all-source intelligence developed by each allied nation. This includes intelligence developed by the various national agencies. National policies must be respected and sources protected. National cells within combined intelligence centers provide for sanitizing sensitive intelligence reports before they are fed into the combined intelligence system.



COMBINED EW STAFF



(1) Naval components below combined level not shown

CHAPTER 14

Logistics

Logistics, the science of moving and maintaining forces and equipment, is critical to sustaining the combat capabilities of any Army unit. It is especially critical to sustaining MI units. The quantities of complex, low-density equipment and the varied operational requirements characteristic of MI units pose an exceptional challenge to logistics support. MI logistics support requirements are satisfied through a combination of internal and external support. This chapter describes the logistics required and the support established to sustain MI tactical operations.

SUPPLY

The objective of supply is the issue of material and equipment to the user. Soldiers must be armed, fed, housed, clothed, and equipped with the items necessary to do their job.

Supply is a complicated, time-consuming task. The closer to the combat zone, the more demanding are the storage and distribution problems. To get required supply items to using units, three methods of distribution are used: supply point distribution, unit distribution, and throughput distribution.

Supply point distribution is that method of distributing supplies in which the receiving unit is issued supplies at a distribution point, the transportation being supplied by the receiving unit. This is the most common distribution method and is used for all classes of supply except class IX and COMSEC items.

Unit distribution is that method of distributing supplies in which the receiving unit is issued supplies in its own area, the transportation being furnished by the issuing agency. This method may be used for any class of supply except COMSEC items; however, it is the exception rather than the rule. Throughput distribution is that method of distributing supplies directly to the consumer. Throughput is the most preferred method of distribution because it allows MI elements to conduct continuous operations.

CLASSES I AND VI

Class I supplies for MI units are obtained through the supply point distribution system. Each MI unit dispatches organic vehicles to pick up rations at the intermediate DS class I supply point. Field rations are obtained in the same manner and retained in the unit supply until needed. The basis of issue is the unit daily strength report submitted through G1 channels.

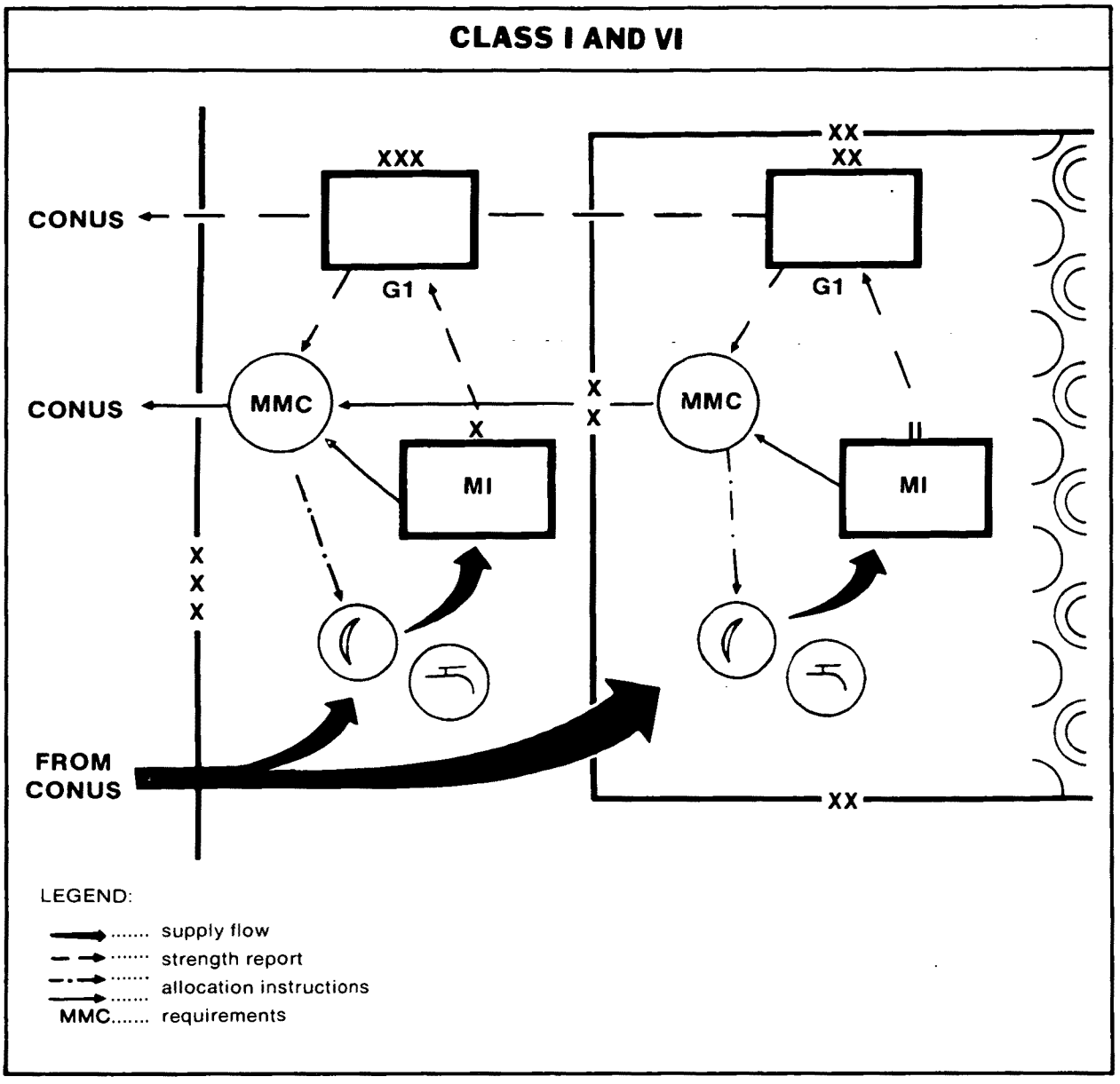
Deployed MI elements depend on units in the forward support area for class I supplies and generally for food service support. Coordination for class I supply and food service support is conducted by the parent MI unit and by the officer in charge of the supporting MI elements.

MI teams attached to maneuver units rely totally on the unit to which attached. The orders directing attachment specify support responsibilities.

Class VI items normally are sold through the Army and Air Force Exchange Service (AAFES). When the situation permits, AAFES establishes retail outlets in combat zones. In other situations, some class VI items are issued as sundry packs in the same manner as class I.

Health and welfare items may be considered class VI supplies and are handled and issued through the supply system. In this case, class I supply points stock and issue health and welfare items as gratuitous issue. Class VI supplies are issued along with class I based on unit strength reports.

An overview of the procedures applicable to classes I and VI supplies is shown in the following illustration.

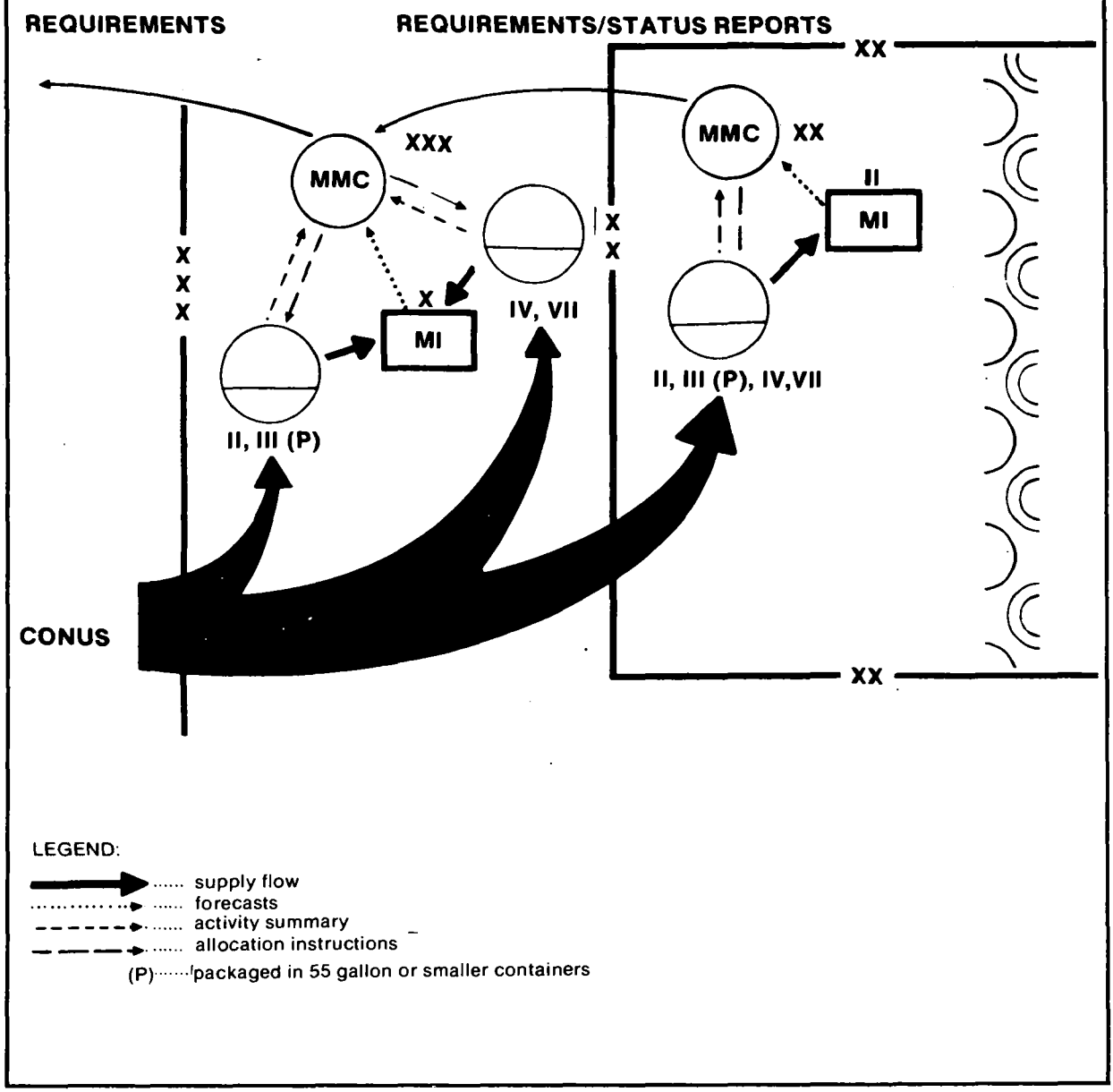


CLASSES II, III (PACKAGED), IV, AND VII

Classes II, III (packaged), IV, and VII have been grouped to expedite issue and simplify handling. At brigade and division level, MI units obtain all four supply classes from one supply point. MI units at corps level receive classes II and III (packaged) from one supply point, while the heavier classes IV and VII items are handled separately. The following illustration outlines the flow of items in these four classes for a typical MI unit.

MI elements operating in maneuver in a brigade area coordinate requirements with the brigade. Supplies are issued by elements of the division support command (DISCOM) main support battalion or forward support battalion. Supply support is tailored to meet the needs of the supported brigade.

CLASSES II, III (P), IV, VII



In an ACR, support for the MI company is normally provided by elements of the ACR support battalion or corps support command (COSCOM).

Deployed elements of an MI unit will coordinate with the nearest supply point and the unit in whose area they are operating.

CLASS III

MI units use fueling points established by elements of the COSCOM in a manner similar to a stateside filling station. MI unit tanker trucks receive POL at the fueling

point and return to the parent unit to service vehicles and generators and refill containers. Deployed MI unit vehicles in forward or rear areas, are driven to and refueled at the nearest fueling point. Attached MI units receive fuel from units to which they are attached. Five-gallon cans or tanker trucks organic to the MI unit are used to move fuel to equipment at dispersed positions.

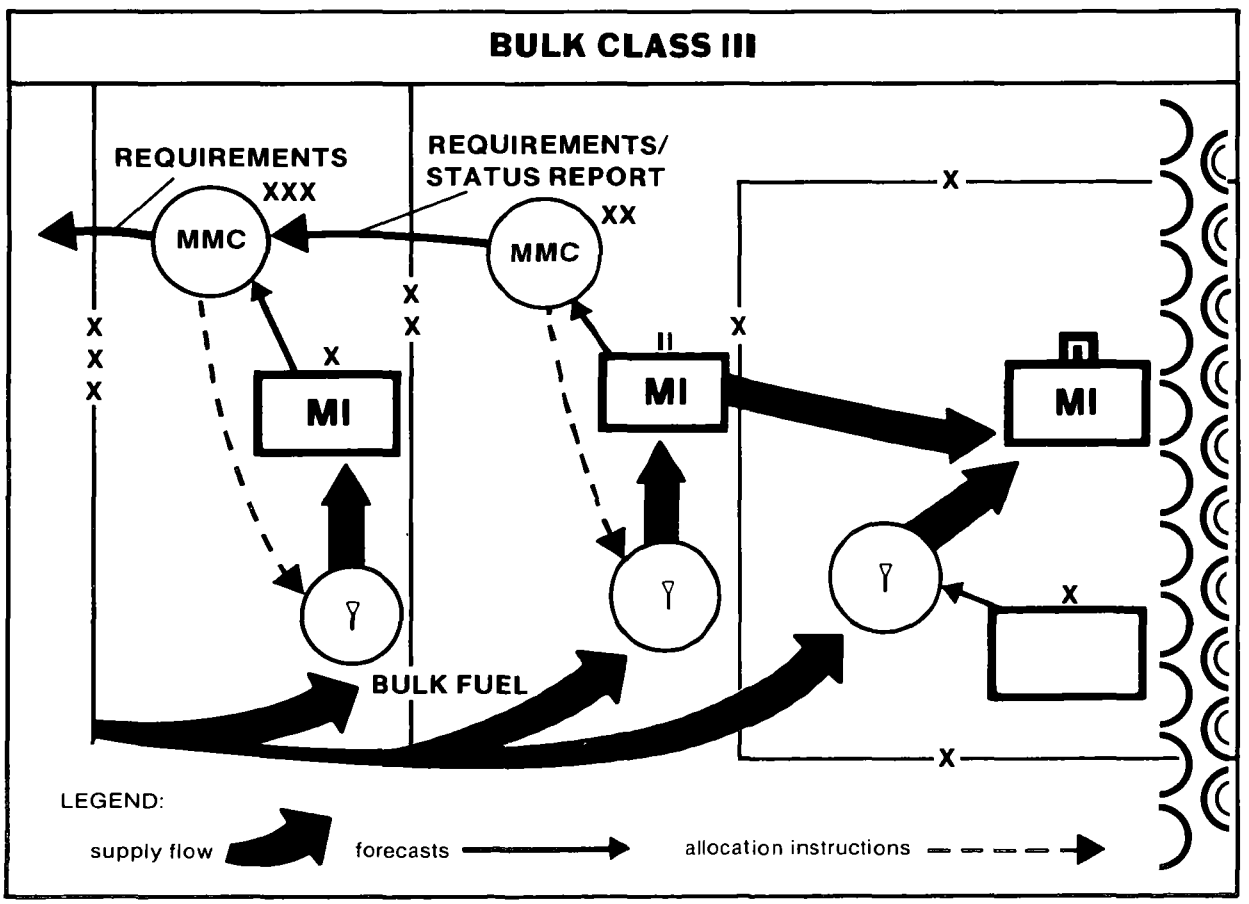
The following illustration shows the flow of bulk class III to MI units.

MI units also have a requirement for aviation POL. Aircraft performing EW missions receive POL support from established airfields and heliports. Helicopters performing MI missions in forward areas may use one of the forward arming and refueling points (FARP) established at a brigade support area or closer to the FLOT.

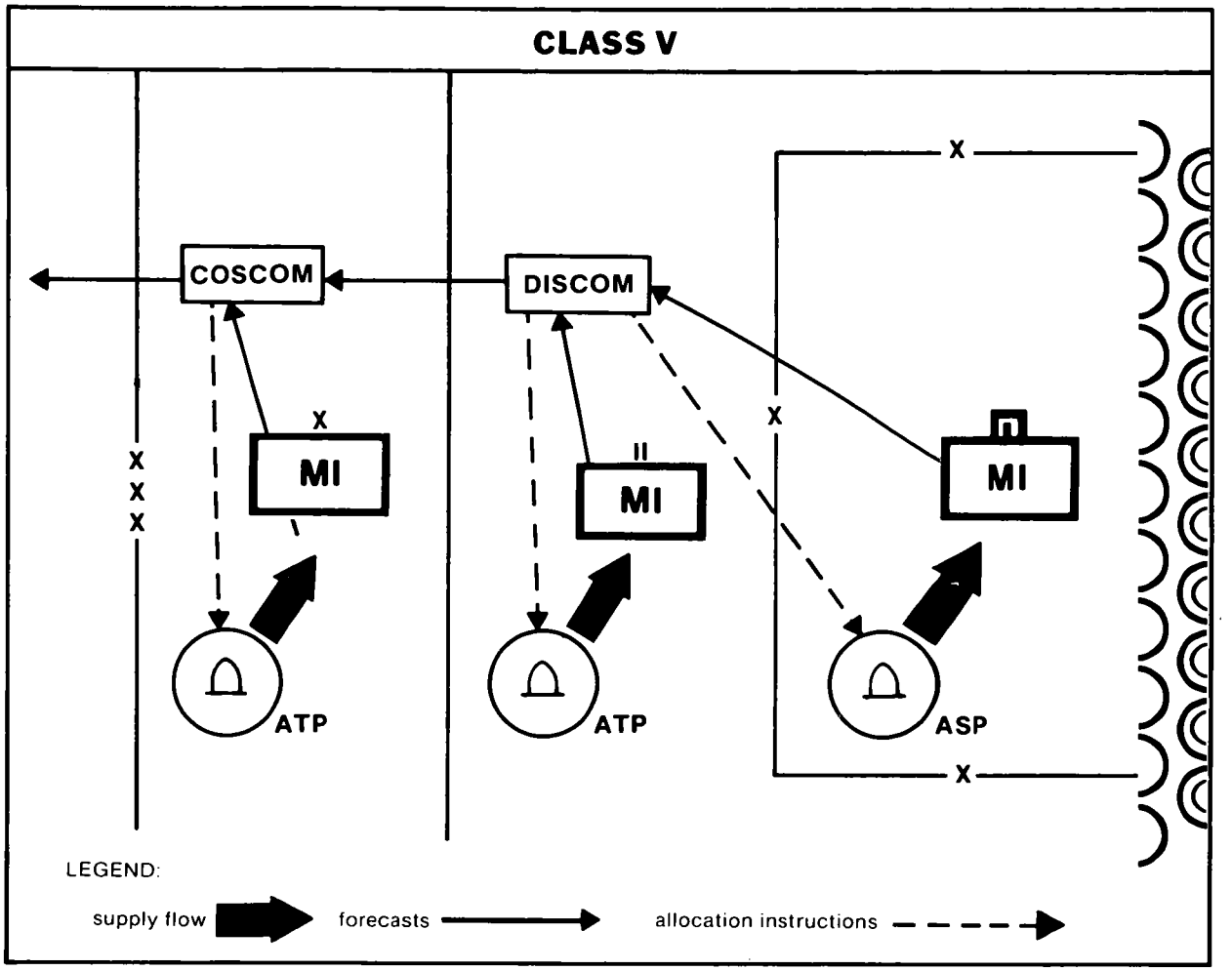
CLASS V

Class V supplies are normally obtained by the supply point distribution system from any ammunition supply activity. The DISCOM monitors requests but does not store or issue class V. The division ammunition officer, assigned to the DISCOM, provides administrative control of the ammunition flow within the division and is the authenticating authority for ammunition requests.

MI units in a division area or brigade sector get class V resupply from a COSCOM ammunition supply point. Class V is allocated by the division ammunition officer who authorizes release by type and quantity based on unit requests. MI elements in a brigade sector are resupplied by the supported unit at ammunition transfer points. Class V on flatbed trailers is positioned in a brigade sector for ready access by using units.



The resupply of class V items is shown in the following illustration.



CLASS VIII

MI units will receive health care or health service support from local medical TOE units on an area basis. These units provide the inpatient and outpatient medical needs for the sick and wounded. Class VIII resupply is provided within the division by the division medical supply officer (DMSO), and within the corps by the medical supply, optical, and maintenance (MEDSOM) battalion. The DMSO is normally located in either the division medical battalion, the main support battalion, or the medical company of the separate brigade. The corps MEDSOM battalion is assigned to the corps under the command and control of the medical brigade or medical group.

CLASS IX

Repair parts may be the most critical aspect of logistic support. The effectiveness of unique MI systems is severely reduced by inadequate repair parts support. Unlike repair parts support for common items, support for systems such as GUARDRAIL and TRAILBLAZER is less readily available because of the low density of such equipment. It is therefore essential that repair parts support be closely monitored by MI commanders and staffs.

The battalion must have on hand or on order a PLL of repair parts, as authorized by the commander. Maintenance is predicated on the principle of on-site repair and

return to operational status with the least possible delay. Repair parts for MI-peculiar equipment are requested by the lowest level authorized to conduct that repair. In most cases involving MI-unique systems, intermediate (DS) is performed by the MI battalion's service support element within the headquarters, headquarters and service company. In such cases, the MI battalion S4 section submits spare parts requests to the Supply Support Activity (SSA). The SSA, if unable to satisfy these requests, passes them to the corps MMC which authorizes the release of parts from the GS supply unit in the corps support group.

Deployed MI elements receive maintenance and repair parts support from the battalion maintenance section organic to the MI battalion. When MI units are task organized into IEW company teams, additional maintenance elements are included in the service support elements of the company organization. Through coordination with the brigade S4, forward-deployed MI elements also may receive common equipment repair parts support from division, ACR, or brigade forward-deployed intermediate (DS) maintenance units.

Controlled exchange, the removal of serviceable parts, components, assemblies, and subassemblies from unserviceable, economically repairable material for immediate reuse in restoring a like item of material is authorized only when the required parts, components, or assemblies cannot be obtained from the supply system in time to meet operational readiness requirements. Controlled exchange is performed by using support maintenance organizations. During periods of combat or transition to combat, MACOM commanders may modify the controlled exchange conditions as deemed necessary. Controlled exchange requirements for using support maintenance organizations are specified in Chapter 4 of AR 750-1.

Cannibalization, the authorized removal, under specified conditions, of serviceable and unserviceable parts, components, and assemblies from material authorized for disposal, supplements supply operations by providing assets not immediately available through the Army supply system. Material awaiting disposition by the National Inventory Control Point will not be cannibalized without specific approval of the proper materiel readiness command or until disposition instructions have been received authorizing local salvage or cannibalization of the materiel. Cannibalization policies and procedures for intermediate and depot maintenance activities are contained in ARs 37-55 and 710-2, and DA Pam 710-2-2.

MI units with aviation assets have organic elements that perform aviation unit maintenance (AVUM). Each AVUM element has a limited number of spare parts and depends on an aviation intermediate maintenance (AVIM) unit for additional spare parts. AVIM units deploy maintenance teams to provide on-site support. Coordination between MI units and the supporting AVIM unit is required on a continuous basis. AVIM units operate from the division rear area, the corps airfield, and from other locations depending on the density of aircraft being supported. Aviation maintenance is further described in this chapter under maintenance. Information on AVIM also may be found in FM 1-500.

The following chart provides more information on aviation repair parts.

OTHER SUPPLY SUPPORT

MI units are staffed and equipped to operate their own dining facilities. MI elements operating in other unit areas coordinate with those units for the support needed.

All units in the field require water for drinking and food preparation. Some MI units also need water for other purposes, such as imagery processing. Elements of the COSCOM locate and develop water sources in the combat zone and supply class I issue points. MI units draw water in bulk from the nearest class I point and transport it to the unit in organic tankers or 5-gallon water cans. Deployed MI elements depend on the supported unit for potable water. Bath and laundry services normally are coupled with clothing exchange. Laundry and clothing exchange are provided by intermediate DS supply units supporting brigades, divisions, and corps.

AVIATION REPAIR PARTS			
UNIT	PERFORMS	RECEIVES	FROM
MI BN (AE)	AVUM	AVIM	Aircraft maintenance battalion element located at corps airfield.
CEWI FLT PLT (OPCON TO MI BN (DIV))	AVUM	AVIM	Aircraft maintenance company located in the division rear.
MI CO (ACR)	AVUM	AVIM	Aircraft maintenance company located in the division rear.

Map coverage of the area of present and projected operations is critical to effective IEW support and tactical operations. Responsibility for the storage and issue of maps rests with the COSCOM or DISCOM supporting MI elements. The MI unit S2 determines unit requirements for maps and coordinates with the S4 for the establishment of a map supply account at the appropriate storage site. Map issue is accomplished by the supply point distribution method.

Since MI units go to war with the personnel they have on hand, personnel replacement is a critical support consideration. During the initial stages of the conflict replacements are provided in accordance with plans worked out in peacetime and based on information gathered in previous combat actions. As current data becomes available, it is reported through S1 or G1 channels and is used to refine and update personnel replacement plans. Replacements are obtained from MI units not committed to combat, from units of the reserve components, and from service schools. Combat loss data also is used as a basis for recruitment and training.

MAINTENANCE, REPAIR, AND RECOVERY

Maintenance is defined as all actions necessary for retaining or restoring an item to a specified condition. It includes inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. It also includes all maintenance related supply actions. The term maintenance includes all repair actions necessary to keep a military force in condition to carry out its mission.

The Army maintenance system is composed of the following levels:

- Unit. User maintenance, which is characterized by quick turn around based on repair by replacement and minor repair (adjust, clean, lubricate, tighten). Maintenance personnel use built-in test equipment to calibrate and isolate defective modules (black box or line replaceable units).
- Intermediate. This category is organized as intermediate (DS) and intermediate (GS). The first is characterized by high mobility, forward orientation, and repair by replacement. Intermediate (GS) maintenance is characterized by semifixed facilities. Its fundamental purpose is to support the theater supply system through repair of components, class VII, and class IX.
- Depot. Maintenance at this level will support the supply system. It will be production-line oriented and will be performed by special repair activities, AMC depots, and contractor personnel.

Though each category is separate and distinct, there are times when a shop performs more than one category of maintenance. The maintenance allocation chart remains the primary tool for assigning specific tasks which can be performed at each category of maintenance. The following chart describes each level of maintenance and who performs that maintenance. It also prescribes the next higher source of repair parts.

LEVELS OF MAINTENANCE

TYPE OF EQUIPMENT	UNIT	INTERMEDIATE MAINTENANCE DS	INTERMEDIATE MAINTENANCE GS	DEPOT
COMMON	HQ HQ & SVC CO, MI BN	FWD SPT BN	TAACOM	AMC CONUS/ HNS
C-E	HQ HQ & SVC CO, MI BN	HQ HQ & SVC CO, MI BN AND FWD SPT BN	TAACOM	AMC CONUS/ HNS
COMSEC	HQ HQ & SVC CO, MI BN	HQ HQ & SVC CO, MI BN AND DIV SIG BN	THEATER CLSU	AMC CONUS/ HNS
RADIAC	HQ HQ & SVC CO, MI BN	MAINT CO (TMDE) DIV SIG BN	MAINT CO (TMDE) COSCOM	AMC CONUS/ HNS
SIGINT/EW	HQ HQ & SVC CO, MI BN	HQ HQ & SVC CO, MI BN	THEATER	AMC CONUS/ HNS
GSR/REMS	HQ HQ & SVC CO, MI BN	HQ HQ & SVC CO, MI BN	THEATER	AMC CONUS/ HNS

VEHICLES, AIR CONDITIONERS, AND POWER GENERATORS

Vehicles, air conditioners, and power generators make up the bulk of items known as common equipment. In the MI battalion, the mechanical maintenance platoon of the headquarters, headquarters and service company provides unit maintenance for this equipment.

Maintenance support teams perform unit maintenance on MI battalion equipment deployed in the brigade areas. They repair the equipment on site whenever possible. Intermediate (DS) maintenance support for common military equipment is also available from maintenance support teams (MSTs) of the forward support battalion which may be under the OPCON of the forward area support coordinator of the supported brigade. Additional maintenance is available from the nondivisional intermediate (DS) maintenance battalion which will provide corps back-up maintenance support.

Maintenance and repair parts support are closely related. Each unit carries its mandatory combat stockage class IX repair parts into combat but must rely on maintenance units for repair parts support. In almost all cases, the unit that provides intermediate (DS) maintenance also provides repair parts support.

COMMUNICATIONS-ELECTRONIC EQUIPMENT

The C-E or IEW maintenance section provides unit and intermediate (DS) maintenance for MI battalion C-E equipment, and COMSEC, EW, GSR, and REMS monitoring equipment. Additional COMSEC unit or intermediate (DS) maintenance requirements are met by the division signal battalion or theater Army COMSEC logistic support units. The platoon maintains a shop stock of repair parts and class IX for the MI battalion in accordance with AR 710-2, DA Pam 710-2-1, and the commander's policy.

FORWARD SUPPORT

When equipment requires repair, battle damage assessments are made by skilled unit maintenance teams. Based on these assessments, every effort is made to repair equipment as far forward as possible to reduce the time required to return it to battle. This is the essence of the forward support maintenance concept.

In most tactical situations, MI assets deploy well forward. Common equipment is repaired by MI unit maintenance contact teams, or if properly coordinated in advance, by maintenance support elements supporting maneuver units. Unique equipment must be repaired by specially trained personnel in the MI unit, or by division or corps maintenance support units.

The MI battalion's forward maintenance contact teams provide maintenance support for deployed MI battalion elements. Additional support—up to intermediate (DS) maintenance—remains with the battalion in the C-E or IEW equipment repair section.

Unit maintenance for SIGINT and EW equipment is performed on site, if possible, by the forward maintenance contact team. If they cannot repair it, it is recovered to the MI battalion trains area and repaired by the C-E or IEW maintenance section. The MI battalion provides intermediate (DS) maintenance support for this equipment. If the MI battalion cannot repair it, it is further evacuated to a TAACOM intermediate (GS) maintenance battalion repair facility.

RECOVERY AND EVACUATION

When on-site repair of MI battalion equipment is not practical due to the tactical situation, the damage involved, or the nonavailability of mobile maintenance teams and when recovery cannot be performed at the platoon level, the headquarters, headquarters and service company will provide special purpose equipment from the MI battalion trains to perform recovery operations. Recovered equipment will be relocated to a unit maintenance collection point, intermediate forward maintenance collection point, or to the brigade support area where damage can be assessed and the repair level determined.

Recovery may also be conducted to retrieve enemy material found on the battlefield which might be of intelligence use. The headquarters, headquarters and service company has the primary responsibility for the task.

Recovered equipment which cannot be repaired at the unit or intermediate DS level will be evacuated by the intermediate (DS) maintenance unit. Evacuation is used to expedite movement of disabled equipment to an activity or maintenance level where repairs can be made.

Prior to evacuation, the maintenance officer considers a controlled exchange of parts according to regulation and command guidance. Systems which have suffered excessive damage may be used as a source of repair parts.

Controlled exchange by using organization is authorized only when—

- Required serviceable parts, components, and assemblies cannot be obtained through maintenance exchange, maintenance (repair and return), or supply channels in time to meet operational readiness requirements.
- All of the unserviceable reparable materiel involved are owned or under control of the organization performing the controlled exchange action.
- The maintenance effort required to restore all of the unserviceable reparable materiel involved to a full mission-capable condition is within the maintenance authority and capability of the organization performing the controlled exchange.
- The unserviceable economically reparable materiel from which the serviceble parts, components, or assemblies are removed is classified not mission-capable supply.
- The action will immediately restore the unserviceable reparable materiel involved to a fully mission-capable condition.
- Such action will not degrade any of the materiel involved to an uneconomically reparable condition.
- It is the only means reasonably available to eliminate an adverse effect on the operational readiness of the unit, organization, or activity performing the controlled exchange.
- All actions are immediately taken to prevent further degrading of materiel from weather or other adverse conditions. The organization performing the controlled exchange will take prompt action to restore the unserviceable materiel to a fully mission-capable condition. The unserviceable part or assembly should be replaced on or retained with the materiel from which the serviceable like item is removed. This is to retain identity and integrity of the reparable materiel.
- Approved by the commander of the organization performing the controlled exchange action.

In those instances where the exchange satisfies a repair parts requirement already due in on requisition through the normal supply system, that requisition will either be canceled or used to restore the remaining unserviceable materiel to a fully mission-capable condition. Requisitions will be processed according to AR 710-2, DA Pam 710-2-1, and DA Pam 710-2-2.

Controlled exchange by support maintenance is authorized only when—

- It is the only means of providing fully mission-capable materiel to a supported unit within the time frame indicated by the issue priority designator code entry on the applicable maintenance request (DA Form 2407).
- It is approved by the shop officer or installation maintenance officer responsible for restoring the not fully mission capable economically repairable materiel involved in the action to a fully serviceable condition.
- The maintenance effort required to restore all of the materiel involved to a fully serviceable condition is within the maintenance authority and capability of the organizations performing the controlled exchange.

- Required serviceable parts, components, and assemblies cannot be obtained on a timely basis through direct exchange or normal supply channels.

Controlled exchange on maintenance floats is not authorized.

Repair parts, components, or assemblies removed in controlled exchange action by support maintenance will be noted on the maintenance request (DA Form 2407), or other appropriate documents for the materiel from which the serviceable items are removed.

AVUM responsibilities for QUICKFIX rests with its parent unit, the aviation brigade. Unit-level repair of EW systems on the QUICKFIX aircraft is performed by 33R personnel assigned to the MI (QUICKFIX) platoon. The MI battalion is responsible for intermediate (DS) maintenance of SIGINT/EW systems on board these aircraft. Since QUICKFIX is OPCON to the MI battalion, if an aircraft is downed during a mission the MI battalion S4 is responsible for notifying the aviation brigade to initiate recovery operations.

MI UNIT MAINTENANCE

MI COMPANY (CEWI) (ACR/SEPARATE BRIGADE)

The MI company (ACR/separate brigade) is similar to, but smaller than, the MI battalion (division). It employs ground and aerial resources and has organic assets to maintain IEW systems. Maintenance on common items such as vehicles; air conditioners; power generators; and radiation, detection, indication, and computation (RADIAC) and COMSEC equipment follows the three-level maintenance system previously described in this chapter.

MI BATTALION (CEWI) (DIVISION)

Maintenance support for the MI battalion (division) is similar to support provided an MI company (ACR/separate brigade) except that intermediate (DS) maintenance support comes from the forward support battalion, and the divisional maintenance battalion. Backup intermediate (DS) maintenance support may be provided by the nondivisional intermediate DS battalion or the corps intermediate GS facility.

When the MI battalion (division) task organizes an IEW company team, it places forward deployed maintenance elements under the command and control of the team commander.

The aviation element is under the operational control of the MI battalion (division) but is organic to the CEWI flight platoon, general support aviation company, which provides AVUM. The division's aircraft maintenance company, a part of the aviation brigade, provides AVIM. The C-E maintenance section of the headquarters, headquarters and service company of the MI battalion provides intermediate (DS) maintenance support for IEW systems.

MI BRIGADE (CEWI) (CORPS)

Maintenance support for the MI brigade (corps) is similar to that for the MI company and battalion. However, that support is complicated by the dispersal of equipment throughout the corps area. Intermediate DS and intermediate GS maintenance and backup support are provided by COSCOM. AVIM is provided by the transportation aircraft maintenance company of the corps support group.

REPLACEMENT

Replacement of IEW peculiar equipment is accomplished through the MMC at division, corps, and EAC. The theater Army MMC requisitions replacements through the appropriate national inventory control points.

CHAPTER 15

NBC Survival and Reconstitution

The capability and willingness of a growing number of nations to employ NBC weapons makes it urgent that US forces plan to fight in an NBC environment. US forces can not allow enemy surprise or first use of NBC weapons to decide the outcome of the conflict. The employment of these weapons drastically alters the traditional concept of fire and maneuver. Their use can rapidly and effectively decide the outcome of the battle.

MI operational objectives are to—

- Survive, operate, and win in an NBC environment.
- Successfully conduct sustained operations under NBC conditions.

Achieving these objectives requires that MI leaders and soldiers fully understand the NBC weapons and the vulnerabilities of IEW systems. It also requires that individual soldiers and teams be well trained and prepared to operate with minimal mission degradation. Prestrike actions include OPSEC measures which help a unit avoid becoming a target. The IEW system may provide the first indications that an NBC attack is imminent and the response time for either a preemptive attack or additional protective measures.

When NBC weapons are used, catastrophic losses may occur in seconds or minutes. Regeneration of combat power must be initiated immediately. The commander will have an immediate need for intelligence on which to base tactical decisions and force reconstitution. With the havoc that can be created by NBC weapons, MI units must recover rapidly for their own survival as well as that of the combined arms team.

EFFECTS

Unit vulnerabilities and defensive measures are dependent upon the effects generated by NBC weapons and agents. IEW force deployment and operations are planned and executed to minimize these effects.

NUCLEAR WEAPONS

Soviet doctrine places great emphasis on the depth, intensity, and destructiveness of an initial nuclear strike. They view this initial massive attack as a means to gain surprise, achieve a major penetration, and destroy effective resistance. The objectives and depth of intended operations will dictate the delivery systems, techniques, yields, and number of nuclear weapons employed. When employed, nuclear weapons are viewed as the primary means of destroying or crippling US forces.

The devastating effects of a nuclear detonation are felt immediately or encountered as a residual hazard. The initial effects create personnel casualties and material damage within the time span of the current operation. The residual effects create long-term problems and impact on maneuverability and survivability within the immediate battle area. The principal initial effects are blast, thermal radiation, initial nuclear radiation, electromagnetic pulse (EMP), blackout, and transient radiation effects on electronics (TREE). Residual effects will include tree blowdown, fire, debris, fallout, neutron-induced patterns, and rainout.

BIOLOGICAL AGENTS

Biological agents are germs or toxins that can be used to cause disease, incapacitation, or death among personnel, animals, or plants and, to a lesser extent, deterioration of materiel. The agents will probably be directed against troops in rear areas; however, some agents may be used in forward

areas when the delay in casualty production due to the incubation period of the agents is not a factor. For more information see FM 3-100.

CHEMICAL AGENTS

Chemical agents are used to kill or incapacitate personnel as well as contaminate terrain and equipment. The contamination of areas and equipment forces extended wear of individual protective equipment which degrades individual and unit performance. In addition, contaminated areas impact on maneuverability. For more detailed analysis of chemical agents and their effects see FM 3-100.

PSYCHOLOGICAL STRESS

One of the most critical problems a commander must deal with following an NBC attack is the psychological impact on personnel. The uncertainty, anxiety, and shock following a nuclear strike can be just as devastating as the strike itself. Unprepared soldiers can become disoriented, confused, and lose their will to fight.

The massive ground attack that will certainly follow an NBC attack will seek to exploit and compound this psychological disorientation. Under such conditions, there will be little time to rebuild confidence and fighting spirit. Preparedness and strong professional leadership are crucial to combating psychological effects while maintaining a coherent fighting capability.

It is well documented that soldiers perform best if they are physically and psychologically prepared for the conditions under which they must perform. Soldiers must know what to expect and what is expected of them. They must understand battlefield conditions as they will face them and practice their skills to proficiency under such conditions.

Because of the very nature of the integrated battlefield, it is not possible to fully replicate the battlefield in a training or exercise environment. The gap between training and reality must be bridged through psychological preparedness. In the chaos of NBC warfare, training provides the knowledge of what must be done; psychological preparedness provides the will to do it.

VULNERABILITIES

All IEW systems and personnel are vulnerable to enemy use of nuclear weapons. Personnel and equipment are also vulnerable to chemical and biological agents in terms of contamination. Survivability is significantly enhanced by the use of protective cover and shielding against the direct effects of a nuclear detonation and the use of protective clothing against chemical and biological hazards.

Electronic systems are also very vulnerable to EMP and TREE damage. EMP and TREE primarily affect electronic and electrical systems and can cause temporary or permanent damage.

EMP is caused by gamma rays stripping electrons off air molecules. This sets up an intense localized electrical field and radiates an extremely strong electromagnetic field. This is picked up by antennas, wire, cables, power leads, internal equipment circuitry, and other metal objects causing overloads. These fields can cause permanent damage or temporary degradation by burning out or degrading components, or by introducing undesirable signals. Modern communications and electronic equipments are sensitive to EMP due to the extensive use of microcircuit transistor technology. The effective range of EMP varies with weapon yield and height of burst.

TREE is caused by neutron and gamma radiation. The radiation degrades electronic components, changing the characteristics of electronic systems. Semiconductors and other solid state components are especially sensitive. Widespread use of radios and other electronic devices by MI units requires extensive protective measures against the effects of EMP and TREE. These measures include disconnecting antennas, cables, and power leads; storing equipment in closed vehicles; insulating electronic equipment; improving employment procedures; and using natural or man-made features for shielding. Specific protective measures for individual items of equipment are covered in appropriate equipment technical manuals.

SURVIVAL

One of the imperatives of air-land battle is to protect the force. On the integrated battlefield, the destructive power of NBC weapons renders personnel and equipment extremely vulnerable to instantaneous destruction. It is therefore critically important that we understand the nature of specific IEW vulnerabilities and be prepared to take appropriate protective measures to ensure survival and continued mission effectiveness.

The basic dilemma facing the commander is how to minimize the risk of NBC destruction while continuing to provide effective MI support. This conflict is resolved based on a risk-benefit analysis that weighs vulnerabilities against mission requirements.

MI units seldom constitute a priority NBC target by themselves. Their primary vulnerability lies in their deployment with or near other forces that are HVTs. Therefore, survivability can be significantly improved by OPSEC helping the supported unit avoid becoming an NBC target. Good OPSEC denies the enemy targeting information and minimizes the risk to combat forces and supporting MI elements alike.

Defense against nuclear weapons effects involves three basic areas: prestrike measures, survival measures, and poststrike measures.

Prestrike measures require an adequate OPSEC posture to preclude detection and targeting by the enemy. This may require some MI units to move more often than in the past. Units will have to streamline their intelligence reporting procedures, and disperse their collection systems. Units must improve their operational techniques and incorporate them into their defense plans and SOPs. This includes EMP protection, hardening of equipment and battle positions, reconstitution plans, and taking advantage of natural terrain features for concealment and cover. For survival, every individual must be trained to immediately take protective action upon attack and afterwards. The unit must be able to recover and continue with the mission. After the attack, the unit must implement reconstitution plans.

Protective measures against living biological agents include immunization and wearing of the protective mask, hood, and gloves. In conjunction with the duty uniform, this ensemble prevents the agents from penetrating the body and causing casualties. For vectors, insect repellants and insecticides are used.

The primary defense against chemical or toxic agents is the implementation of mission-oriented protective posture (MOPP). The commander weighs the extent of the chemical threat, mission, work rate, and heat stress involved and then specifies the MOPP to complete the mission with minimum casualties. The choice of MOPP ranges from no protection to full protective clothing and equipment. Higher levels of MOPP increase the incidence of heat exhaustion and fatigue which degrade individual efficiency. The choice of MOPP minimizes chemical casualties while still providing for mission accomplishment.

Personnel and equipment survivability is greatly enhanced through the use of protective measures as described in FMs 3-100 and 3-4. FM 3-100 also provides an example of an NBC defense annex to a unit SOP that is readily adaptable to MI operations. Additional actions that MI units may take to reduce vulnerability and provide for continuity of operations when an NBC strike is imminent include—

- Further dispersing resources, to include command and control and processing facilities.
- Moving selected systems to hardened battle positions.
- Moving selected portions of the MI unit operations center and TOC support element to more hardened battle positions when a nuclear strike warning is issued.
- Taking protective measures for selected systems and personnel.
- Changing the designated MOPP, if applicable.

- Providing contingency tasking, intelligence, and technical information to MI elements to provide for limited independent poststrike operations.

DECONTAMINATION

Contamination is a problem because it can kill or injure soldiers, or, as a minimum, degrade their ability to fight by forcing them to MOPP 4. Protective clothing and shelters are only temporary solutions. Decontamination is the solution. Decontamination is the removal, destruction, or neutralization of contamination. There are four practical reasons for conducting decontamination:

- Contamination can be lethal to unprotected soldiers.
- MOPP gear degrades a soldier's performance.
- MOPP gear has limitations.
- Contamination tends to spread.

There are three types of decontamination: basic soldier skills, hasty, and deliberate:

- ***Basic soldiers skills*** consist of skin decontamination, personal wipedown, and operator's spraydown. A soldier must be able to perform these techniques automatically to sustain life.
- ***Hasty decontamination*** allows a force to fight longer and sustain its mission while contaminated. The techniques of MOPP gear exchange and vehicle washdown allow for removal of gross amounts of contamination. Hasty decontamination should be done as soon as practical.
- ***Deliberate decontamination*** is done as part of an extensive reconstitution effort in brigade, division, and corps support areas. Detailed equipment and troop decontamination is conducted by the contaminated unit with assistance from the chemical unit.

DEPLOYMENT

MI resources routinely are dispersed throughout the battlefield to make maximum use of their capabilities. When preparing for operations on an integrated battlefield, MI commanders may alter the deployment profile to increase the survivability of selected systems. Within the constraints of the current situation and the mission, they select the deployment profile that provides the best probability of mission success and survivability.

This involves a risk assessment that balances IEW system vulnerabilities against the need to accomplish the mission and continue operations. It centers on enemy capabilities and intentions and the need to protect specific capabilities and systems from destruction. It is a continuous process, changing with the situation and updated knowledge of the enemy.

The operational profile of MI units is designed to enable each element to operate to its fullest potential. Changing this profile to increase survivability on an NBC battlefield generally results in some elements operating at less than full potential because of range, LOS, or other system limitations. Profile options that increase survivability include—

- Stand off coverage by aerial resources in lieu of ground-based systems.
- Deploying critical systems to low threat areas where they operate at their range limits.
- Emphasizing survivability over mission capability when employing systems within high threat areas.
- Remote operation of systems.
- Relying on unmanned devices in highest threat areas. This option will increase in importance as additional unmanned systems such as drone aircraft, robotics, Remotely Monitored Battlefield Sensor System (REMBASS), and expendable jammers enter the inventory.

Based on projected enemy use of NBC weapons, MI commanders determine the capabilities they could lose to such an attack. They assess the impact of the lost capability on future operations and determine if additional protective measures are required. If such measures would degrade

current operations, commanders may—

- Accept the risk and continue operations.
- Request higher headquarters support.
- Operate at reduced capability.
- Change the profile of the unit.

RECONSTITUTION

Reconstitution is the regeneration of the force with people, organization, C^2, and equipment. It may be accomplished through individual item or personnel replacement, the combining of units or functions, or continuing operations at reduced strength and capability. Reconstitution consists of short- and long-term actions.

Short-term actions are taken immediately after an NBC strike, and are aimed at regenerating combat power from surviving resources. They are keyed to the immediate tactical situation and the commander's most urgent IEW needs. Priority of effort is directed toward those IEW resources needed to collect against, report on, and assist in countering the immediate threat—essentially enemy first-echelon forces that can be committed up to about 18 hours following the strike. A much greater reliance on EAC, other services, and national assets will be necessary to meet the commander's intelligence requirements.

Long-term actions are those taken to fully assess the extent of losses and to acquire the personnel and equipment needed to restore full operating capability. They are keyed toward IEW support of the long-range plans of the command. Replacements may be available from higher headquarters or adjacent units, but this will depend upon availability and an assessment of enemy intentions. In both long- and short-term situations, IEW support may be available from higher and adjacent commands on a mission or priority of effort basis.

PLANNING

Planning and preparation are essential to rapid and effective reconstitution. SOP or contingency plans are developed to guide both long-and short-term reconstitution actions. They provide clear and detailed

Closely allied with C^2 in MI units is the capability to process information and direct resources to effectively provide IEW support. When such capabilities are lost, they too must be replaced immediately. Alternatives include reconstituting with personnel instructions for actions required at each echelon. At a minimum, they provide instructions on—

- Replacing lost C^2.
- Primary and alternate means of communication to include skip echelon.
- Mission profiles for different threat intensities.
- Limits of independent operations.
- Reporting of status and needs.

Greater reliance on EAC and national assets for operations during and after nuclear strikes includes the need for equipment repair or replacement, personnel fill, and data base replacement as well as continued information flow.

COMMAND AND CONTROL

Regenerating C^2 is critical to restoring effective, responsive functioning of the IEW system. Command and control provide the means for reorganizing and redirecting surviving assets, assessing the extent of losses, determining reconstitution requirements, and initiating reconstitution actions.

If the C^2 of an MI unit or element is lost or rendered ineffective, it should be reinstituted immediately. SOP or plans should clearly state the manner of replacement. Alternatives include a backup CP, assumption of command by a preselected subordinate commander, or insertion of a capability from higher headquarters.
and equipment from other elements or reassigning the responsibility to another element which possesses the necessary capabilities. Personnel expertise, communications, and existing data bases are primary considerations. Centralized operations should be reestablished as quickly as possible for unity in coordinating, cuing, and applying various IEW assets.

Rapid reconstitution of C^2 requires a concerted effort by all echelons within the IEW system. Each must use whatever means

available to reestablish communications with both superiors and subordinates. Skip-echelon communications may be necessary to bypass an echelon that is no longer functioning.

The wide dispersal of MI units and teams across the battlefield creates severe C^2 problems. Many MI elements will be cut off from their controlling headquarters for varying lengths of time. Because much of the IEW mission is executed by these elements, it is urgent that they continue to operate while the control system is being reestablished.

Continued operation requires that tasking be evaluated in light of the current situation unless specific poststrike tasking has been established. A decision is made whether to continue current tasks or change to tasking that better suits the situation. Such alternatives must be fully covered by SOP or plan to provide the element leader with a clear statement of poststrike IEW objectives on which to base decisions.

Isolated MI teams should establish contact with nearby maneuver units and provide them with IEW support until the IEW command and control system is regenerated and centralized control is reestablished. When doing so, the team leader explains the type of support that can be provided and assists the commander or S2 in using that support.

REGENERATION

Regenerating the IEW system to full mission capability is essentially a long term operation. It begins with an assessment of the situation to determine the extent of losses and the amount and type of reconstitution required. Initially, this may be only a prediction by the staff based on element locations and ground zeroes. As detailed information or poststrike analysis on personnel and equipment losses and repair parts needed becomes available, the assessment is revised.

Regeneration normally involves removing a severely depleted unit from its present mission status; however, MI units are regenerated in place when possible. Personnel and equipment are moved forward to replace losses and enable units to continue operations. Repair and decontamination are performed as far forward as the situation permits.

Personnel replacements are provided based on losses reported through G1 or S1 channels. Because many MI skills are unique, replacement personnel may not be readily available. Immediate replacements will be drawn from other MI units within the theater of operations based on the mission and priorities of the units concerned. On a long-term basis, these personnel requirements may be filled from CONUS-based units, other overseas units, the reserves, and the training bases.

Initial regeneration of equipment will focus on the repair of lightly damaged equipment to return it to service as quickly as possible. Degraded communications, decontamination requirements, and the need to avoid heavily contaminated areas will seriously hamper maintenance and supply operations. Cannibalization may be required until the supply system can catch up with the demand for parts. Major equipment items needed to replace losses are requested through command channels.

The IEW mission in an NBC environment remains the same as for a conventional battlefield. That mission is to provide timely, accurate intelligence; effective CI support; and a responsive EW capability to the commander. Accomplishing this mission depends on planning, the SOP, the general defense plan, and centralized control at the MI unit operations center level. Communications difficulties and the dispersal of units characteristic of a nuclear battlefield will make control difficult. It requires careful planning and a full understanding of IEW system capabilities and limitations.

Survivability is directly dependent on the positioning of resources and the protective measures taken. The commander decides how and where to employ resources based on an assessment of risk and missions assigned. The operational profile may be vastly altered to enhance survivability.

Reconstitution efforts immediately following a nuclear strike focus on rapidly regaining maximum mission capability with surviving resources. Further efforts are directed at fully regenerating all IEW capabilities.

APPENDIX A

The Analysis of the Battlefield Area

An analysis of the battlefield area is made to determine its effect on the enemy and friendly force's courses of action. Considerations for the analysis are:

- ☐ Climate and weather conditions.
- ☐ Relief and drainage systems.
- ☐ Vegetation.
- ☐ Surface materials.
- ☐ Man-made features.
- ☐ Military aspects of the area.
- ☐ Observation and fire.
- ☐ Concealment and cover.
- ☐ Obstacles.
- ☐ Key terrain.
- ☐ Avenues of approach (air and ground).
- ☐ Other effects of the area on combat service support operations.

Additional considerations are:

- ☐ Sociological.
- ☐ Political.
- ☐ Economic.
- ☐ Religious.
- ☐ Scientific.
- ☐ Technological.
- ☐ Materiel.
- ☐ Transportation.
- ☐ Hydrography.

The analysis of the battlefield area is a critical product of the G2's activities.

The G2 has primary staff responsibility for initiating, coordinating, and ensuring completion of the analysis. Other staff sections contribute within their respective fields. Primary contributions include—

- ☐ The engineer's terrain study.
- ☐ The SWO climatological studies and weather forecasts.
- ☐ The civil-military operations or G5's information on sociology, politics, economics, psychology, technology, and local labor conditions.
- ☐ The unconventional warfare officer's information from areas not under the control of friendly forces.

The G2 uses other sources such as area studies, periodicals, the US Army Institute for Military Assistance, DIA, and the CIA to prepare the analysis of the battlefield area.

The analysis of the battlefield area is begun well in advance of hostilities. It focuses on each contingency area for which the command is tasked or anticipates tasking. IPB is facilitated by the initial data gathering done for the analysis of the battlefield area. Once the initial data gathering is accomplished, IPB proceeds concurrent with the preparation of the analysis of the battlefield area, with each contributing to the other. The G2 ensures that there is no duplication of effort between the analysis of the battlefield area and IPB. The terrain and weather analyses accomplished in IPB, can provide data which will fully support paragraphs 2a, 2b, and 3a of the analysis of the battlefield area (see the example in this appendix). When the prehostility IPB analysis nears completion, the G2 uses all available data and analyses to determine the effects of the characteristics of the battlefield area on both friendly and anticipated enemy courses of action.

On receipt of an order to implement a contingency plan, the intelligence officer reevaluates the analysis. After the commander has reached a decision and issues a concept of operations, the analysis of the battlefield area may require refinement because of the adopted course of action. As the operation progresses, new battlefield areas are assigned and changes in mission

or recipt of additional or more accurate information may require a revision of the analysis of the battlefield area.

A written analysis is usually completed only at corps and EAC to support projected operations. At division, a written analysis may be prepared for projected operations (such as airborne operations) to be carried out at great distances. Most division operations, however, will use the corps analysis of the battlefield area supplemented by IPB information pertinent to the division.

FM 101-5 presents the format including a general description of the content of each element. A brief outline of the format follows.

ANALYSIS OF THE BATTLEFIELD AREA

1. PURPOSE AND LIMITING CONSIDERATIONS.

2. GENERAL DESCRIPTION OF THE AREA.

a. Climatic or Weather Conditions.

b. Terrain.

(1) Relief and drainage systems.

(2) Vegetation.

(3) Surface materials.

(4) Man-made features.

c. Additional Characteristics.

3. MILITARY ASPECTS OF THE AREA.

a. Tactical Aspects.

(1) Observation and fire.

(2) Concealment and cover.

(3) Obstacles.

(4) Key terrain features.

(5) Avenues of approach.

b. Combat Service Support Aspects.

(1) Personnel.

(2) Logistics.

(3) Civil-military operations requirements.

4. EFFECTS OF CHARACTERISTICS OF THE AREA.

a. Effect on enemy courses of action.

b. Effect on own courses of action.

Paragraph 2 of the intelligence estimate contains an abbreviated version of the analysis of the battlefield area. Whether the analysis of the battlefield area is in written format or briefed verbally, all the information required in paragraphs 1 through 4 of the format must be presented.

APPENDIX B

The Intelligence Estimate

The intelligence estimate is a logical, orderly examination of the intelligence factors affecting the mission. Its main purpose is to determine the courses of action open to the enemy commander and the probable order of their adoption. It provides an analysis of the AO, and information on enemy strength, capability and vulnerability. It is a basis for planning operations and disseminating intelligence.

(Classification)

Headquarters
Place
Date, time, and zone

INTELLIGENCE ESTIMATE NO. _____

References: Maps, charts, or other documents.

1. MISSION
The restated mission determined by the commander.

2. THE AREA OF OPERATIONS
This paragraph discusses the influence of the AO used in arriving at conclusions. It is based on the facts and conclusions of IPB and the analysis of the AO, if one has been prepared. It may be a reference to an analysis of the AO, if adequate coverage and discussion are contained therein.

a. Weather.

(1) Existing situation. Include light data and either a weather forecast or climatic information, as appropriate. Use appendixes for detailed information.

(2) Effect on enemy courses of action. Describe the effects of weather on each broad course of action (e.g., attack, defend). Each description concludes with a statement of whether the weather favors the course of action. Among the courses of action, include use of chemical agents; nuclear weapons; and special methods, techniques, equipment, procedures, or forces.

(Classification)

(Classification)

(Short title identification)

(3) Effect on own courses of action. Describe in the same manner as for (2) above, except that the estimate excludes the use of biological agents.

b. Terrain.

(1) Existing situation. Use graphic representations such as IPB templates where possible. Use annexes for detailed material. Include as much information as necessary for an understanding of observation and fire, concealment and cover, obstacles, key terrain features, and avenues of approach. Include effects of nuclear fires, enemy biological and chemical agents, and any other pertinent considerations on each of these factors as appropriate.

(2) Effect on enemy courses of action. Describe in the same manner as for the effects of weather in a(2) above. For defensive courses of action, state the best defense area and the best avenues of approach leading to it. For attack courses of action, state the best avenues of approach.

(3) Effect on own courses of action. Describe in the same manner as for effects of weather in a(3) above.

c. Other Characteristics. The following additional characteristics considered pertinent are included in separate subparagraphs: sociology, politics, economics, psychology, and other factors. Other factors may include such items as science and technology, materiel, transportation, manpower, and hydrography. These factors are analyzed using the same subheadings as weather and terrain.

3. ENEMY SITUATION

This paragraph gives information on the enemy which will permit later development of enemy capabilities and vulnerabilities and refinement of these capabilities into a specific course of action and its relative probability of adoption.

a. Disposition. Reference may be made to overlays, enemy situation maps, or previously published documents.

(Classification)

b. Composition. Summarize enemy order of battle that can influence accomplishment of the mission. Reference may be made to previously published documents. Special mention is made of units capable of EW, low-intensity operations, and other special operations, as appropriate.

c. Strength. Enemy strength is listed as committed forces, reinforcements, air, nuclear weapons, and chemical and biological agents. The purpose of this listing is to assist in developing enemy capabilities and vulnerabilities for use by the commander and staff in selecting courses of action. The unit mission, location of the enemy, enemy doctrine, and the level of command at which the estimate is being prepared are factors to be considered.

(1) Committed forces. List those enemy ground maneuver units currently in contact and those ground maneuver units with which imminent contact can be expected regardless of the specific friendly course of action implemented. Designation of enemy forces as committed forces depends on disposition, location, controlling headquarters and doctrine. The intelligence officer usually accounts for committed forces based on the size unit doctrinally used to oppose the friendly unit. Generally, enemy units are counted in terms of units two echelons below the friendly unit's size (e.g., a brigade S2 normally considers committed forces in terms of companies; a division G2, in terms of battalions; and a corps G2, in terms of regiments). If there is doubt whether a unit is a committed force or a reinforcement, it is considered a reinforcement. This attributes to the enemy the maximum capability to reinforce forces to oppose a given friendly course of action.

(2) Reinforcements. Include designation and location. Reinforcements are those enemy maneuver units that may or may not be employed against us, depending on our choice of a specific course of action and enemy plans. Reinforcements are enemy units not committed in or out of the friendly sector, but which can react to the friendly course of action, subject to time and distance considerations, in time to influence the accomplishment of the mission. Imminent contacc is not expected. Disposition, location, level of control, or other factors at the time of the estimate are considered in determining wnich enemy forces are reinforcements.

(3) Air. List the number of enemy aircraft by type within operational radius. Include the number of possible sorties per day by type of aircraft, if known.

(4) Nuclear weapons and chemical and biological agents. Estimate, as appropriate, the number, type, yield, and delivery means of enemy nuclear weapons and chemical and biological munitions or agents available to the enemy.

d. Recent and Present Significant Activities. List selected items of information to provide bases for analyses to determine relative probability of adoption of specific courses of action and enemy vulnerabilities. Enemy failure to take expected actions are listed as well as positive information.

e. Peculiarities and Weaknesses. Based on knowledge of enemy tactical doctrine, practices, the principles of war, the AO, and the enemy situation previously described and discussed, list peculiarities and weaknesses and briefly describe each, indicating the extent to which they may be vulnerable and how they influence possible friendly courses of action. The items listed are grouped under the headings indicated below. Only pertinent headings are used.

(1) Personnel. An estimate of strength usually is included if less than 80 percent of authorized strength. Status of morale is included, if known.

(2) Intelligence. An estimate of enemy intelligence success, ineffectiveness, and susceptibility to deception and detection usually is included.

(3) Operations. An estimate of combat effectiveness usually is included if less than excellent.

(4) Logistics. An estimate of the enemy's capability to support their forces logistically is included if there are apparent weaknesses.

(5) Civil-military operations. An estimate of the attitudes of the enemy and the civilian populace and the status of food supply, medical facilities, communications, and other critical resources usually is included.

(6) Personalities. An estimate of the capabilities and weaknesses of the enemy commander and principal staff officers usually is included.

4. ENEMY CAPABILITIES

Based on all the previous information and analyses, develop and list enemy capabilities. The listing provides a basis for analyzing the available information to arrive at those capabilities the enemy can adopt as specific courses of action and their relative probability of adoption.

a. Enumeration. State what, when, where, and in what strength for each capability.

b. Analysis and Discussion. To provide a basis for conclusions of enemy capabilities and their relative probability of adoption, each capability, or appropriate combination thereof, is discussed in a separate subparagraph. Consideration of enemy deception measures is included. All the pertinent previous information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the enemy point of view of whether the adoption of the capability is advantageous to the enemy. Such judgements need not be made if the conclusion is obvious or if there is no evidence that the enemy will adopt the capability, except when the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

5. CONCLUSIONS

Based on all the previous information and analyses, conclusions are stated concerning the total effects of the AO on friendly courses of action; the courses of action most likely to be adopted by the enemy, including their relative probability of adoption; and the effects of enemy vulnerabilities that can be exploited. These conditions assist in the selection of a friendly course of action.

(Classification)

(Short title identification)

a. Effects of Intelligence Consideration on Operations. Indicate whether the mission set forth in paragraph 1 above can be supported from the intelligence standpoint. Indicate which course(s) of action can best be supported.

b. Effects of the AO on Own Courses of Action. For attack courses of action, indicate the best avenues of approach. For defensive courses of action, indicate the best defense areas and the best avenues of approach leading to and into the defense areas. (This subparagraph is omitted if the discussion of the effects of the area on own courses of action in paragraph 2 has been omitted because of the availability of a current analysis of the AO.)

c. Probable Enemy Courses of Action. List courses of action in order of relative probability of adoption. A listed course of action may include several subordinate courses of action that can be executed concurrently. Usually, no more than two or three courses of action, in order of probability of adoption, can be justified by the available evidence.

d. Enemy Vulnerabilities. List the effects of peculiarities and weaknesses that result in vulnerabilities that are exploitable at own, higher, or lower levels of command. The order in listing these vulnerabilities has no significance.

/s/ _____
(Designation of staff officer)

Annexes (as required)

(Classification)

APPENDIX C

The Intelligence annex

This appendix implements STANAG 2014 (Edition Five)

The intelligence annex is an integral part of any operation plan or order. The purpose of the annex is to provide details not incorporated into the basic order. The annex should be as brief as possible yet provide sufficient information to accomplish the mission. It is used to keep the basic text of the order short and allows the selective distribution of its contents. The annex is used to disseminate PIR, IR, and intelligence tasks.

The intelligence annex provides information and direction to subordinate units of the command. It is usually prepared at division and above by the G2 supported by the ASPS and CM&D section. It is unique among annexes in that it has provisions for requesting information from higher and adjacent units needed to support the unit collection plan.

(Classification)

Copy no. _____ of _____ copies
Issuing headquarters
Place of issue (may be in code)
Date/time group of signature
Message reference number

(Short title identification)

ANNEX _____ (INTELLIGENCE) TO OPERATION ORDER NO _____
References: Maps, charts, and other relevant documents.
Time zone used throughout the order:

1. SUMMARY OF ENEMY SITUATION

Information about enemy forces essential to implementing the operation plan. When the amount of detail makes it appropriate, a brief summary and reference to the appropriate intelligence document or appendix to the annex may be used. Reference to documents not included in the annex should not be made when they are not available to all recipients of the annex.

(Classification)

(Classification)

2. INTELLIGENCE REQUIREMENTS

List each PIR in priority order, in a separate subparagraph. The fact that they are in priority order should be made clear. In a final subparagraph, list other intelligence requirements, if any.

If an intelligence annex is not prepared or is distributed separately from the basic order, PIR should be listed in the coordinating instructions subparagraph of the operation order.

3. INTELLIGENCE ACQUISITION TASKS

a. General. Common collection tasks and NAIs of concern to the issuing headquarters are listed.

b. Orders to subordinate and attached units. Detailed instructions for reports required by the issuing headquarters are listed, by unit, in a separate numbered subparagraph. Units are listed in the same order as they are listed in the operation order.

c. Requests to higher, adjacent, and cooperating units. List requests for information from units not organic or attached in a separate numbered paragraph.

d. If publication of an intelligence annex is deferred or omitted, the intelligence and information requirements are put in the coordinating instructions subparagraph of the OPORD. They are not, however, published in both places except when the commander desires that certain requirements be emphasized.

4. MEASURES FOR HANDLING PERSONNEL, DOCUMENTS, AND MATERIEL

This paragraph contains instructions pertaining to the operation not contained in SOP or which modify or amplify SOP for the current operation. For example:

a. Prisoners of war, deserters, repatriates, inhabitants, and other persons. Special handling and segregation instructions.

b. Captured documents. Instructions for handling and processing of captured documents from time of capture to receipt by specified intelligence personnel.

c. Captured materiel. Designation of items or categories of enemy material requirements for acquisition and examination, and specific instructions for its processing and disposition.

(Classification)

(Classification)

5. DOCUMENTS OR EQUIPMENT REQUIRED

This paragraph lists, in each category, the conditions under which certain documents or equipment required by or allocated to units to execute their intelligence collection requirements can be obtained or requested. This includes routine requirements for maps.

6 COUNTERINTELLIGENCE

a. This paragraph is covered largely by SOP. Many special operational instructions having counterintelligence aspects are listed in the operation order or in other annexes.

b. Certain instructions and procedures pertaining to the operations of special personnel may require limited dissemination on a "need to know" basis. Therefore, a "Special Counterintelligence Measures" appendix may be prepared for a limited and specified number of addressees.

7. REPORTS AND DISTRIBUTION

This paragraph may be covered largely by SOP. It stipulates the conditions (dates, number of copies, issue, etc.) regulating the issue of intelligence reports to the originating command for the duration of the operation. Any or all of the following items may be covered in this paragraph:

a. Periods to be covered by routine reports and distribution.

b. Routine and special reports which differ from SOP required from subordinate units.

c. Periodic or special conferences of intelligence officers.

d. Distribution of special intelligence studies, such as defense overprints, imagery intelligence reports, and order of battle overlays.

e. Special intelligence liaison when indicated.

8. MISCELLANEOUS INSTRUCTIONS (if required)

List here, under special subparagraphs, necessary items not covered above or in SOP, or which require action different from that detailed in SOPs.

Acknowledgement instructions.

(Classification)

(Classification)

Last name of commander
Rank

Authentication.

Appendixes:

Distribution:

(Classification)

APPENDIX D

The Electronic Warfare Estimate

The EW estimate is designed to assist the staff officer in considering recommended courses of action for accomplishing a specific task, providing the commander a sound basis for decision making. The estimate is as thorough as time and circumstances permit. It may be written or verbal depending on the level of command involved. In either case, a logical systematic approach is required. The estimate will show the commander how his maneuver courses of action can be supported by EW or will be affected by enemy EW conducted against friendly C-E systems.

Because of the broad scope of EW, it is essential that information, conclusions, and recommendations from other pertinent estimates be used in developing the EW estimate. Close coordination with intelligence, operations, and C-E staff activities is essential. FM 101-5 and FM 34-40 (S) contain information on the EW estimate.

(Classification)

Copy no. _____ of _____ copies
Issuing headquarters
Place of issue (may be in code)
Date/time group of signature

ELECTRONIC WARFARE ESTIMATE NO. _____
References: Maps, charts, and other relevant documents.
Time zone used throughout:

1. MISSION
   This paragraph states the general mission of the command.

2. SITUATION AND COURSES OF ACTION
   a. Considerations affecting the possible courses of action.
      (1) Characteristics of the AO.
          (a) Weather.
          (b) Terrain.
      (2) Enemy EW situation.
      (3) Own EW situation.
      (4) Relative EW combat support power.
      (5) EW resources used.
      (6) EW support to other plans.

(Classification)

(Classification)

(Short title identification)

b. Enemy capabilities.
   (1) Enumerated EW capabilities
   (2) Enemy probable course of action and effect on EW.
   (3) Enemy EW vulnerabilities.
c. Friendly EW vulnerability.
d. Own courses of action.

3. ANALYSIS OF OPPOSING COURSES OF ACTION

4. COMPARISON OF OWN COURSES OF ACTION

This paragraph compares maneuver courses of action by listing EW support and C-E protection advantages and disadvantages derived from paragraph 3.

a. Course of Action.
   (1) Advantages.
   (2) Disadvantages.
b. Discussion.

5. RECOMMENDATION

This paragraph translates the "best" course of action as determined in paragraph 4 into a complete recommendation outlining who, what, where, when, how, and why from the EW and C-E point of view. It states which maneuver course of action will best be supported by friendly EW as well as how it can be supported and protected. The recommendation should point out how much less vulnerable the friendly force will be to enemy EW.

/s/_____

ANNEXES: (Include annexes as required. Annexes with pertinent details, should be used to the extent practical to support the contents of the estimate. These annexes may be in considerable detail with only the high point included in the body of the estimate. Annexes should add depth to the contents of the body and not be used as a substitute. Key points, those having a direct bearing on the problem, must be included in the body of the estimate at the expense of brevity.)

(Classification)

APPENDIX E

The Electronic Warfare Annex

This appendix implements STANAG 2014 (Edition Five)

The EW annex is usually an integral part of an operation plan or order prepared at division level or higher. Its purpose is to provide detail not readily incorporated into the basic order. It also allows the selective distribution of EW information.

Information pertaining to operation plans, orders, and annexes is found in FMs 101-5 and 34-40 (S).

(Classification)

(Change from verbal orders, if any)

Copy no. _____ of _____ copies
Issuing headquarters
Place of issue (may be in code)
Date/time group of signature
Message reference number

ANNEX _____ (ELECTRONIC WARFARE) to OPERATION ORDER NO _____
References: Maps, charts, and other relevant documents.
Time zone used throughout the order:

1. SITUATION

Items of information affecting EW operations not included in paragraph 1 of the operation order or which need to be expanded.

a. Enemy forces. Provide information about those enemy forces capable of affecting the mission upon which the overall plan is based. Reference may be made to the intelligence annex.

(1) Major elements. Identify major enemy commands that will exercise command and control in the coming battle.

(2) Enemy electronic systems. Provide information on electronic doctrine employed by the major elements listed in paragraph 1.a. (1) above. Known deviations from doctrine should be included.

(Classification)

(Classification)

(Short title identification)

(3) Enemy radio electronic combat. Provide information on the employment of REC resources against US and allied forces. Identify the US and allied targets of REC operations.

b. Friendly Forces:

(1) Outline higher headquarters plan.

(2) Outline higher and adjacent unit EW plans.

(3) Note additional EW resources supporting the unit.

c. Attachments and Detachments. EW resources attached and detached to include effective times, if applicable.

2. MISSION

A clear, concise statement of the EW task.

3. EXECUTION

a. Concept of Operation. A brief statement of the EW operations to be carried out to include priorities.

b. EW Tasks to Subordinate and Supporting Units.

c. EW Tasks to Subordinate and Supporting Units.

d. EW Tasks to Subordinate and Supporting Units.

e. Coordinating Instructions:

(1) Instructions applicable to two or more subordinate units.

(2) Reference to supporting appendixes not referenced elsewhere in the annex.

(3) Reference to other annexes necessary for coordination of EW operations (deception, C-E, psychological operations).

4. SERVICE SUPPORT

This paragraph contains a statement of the instructions and arrangements supporting EW operations.

5. COMMAND AND SIGNAL

This paragraph contains instructions relative to command and to C-E in support of EW operations. There are usually two subparagraphs.

a. Command. List the location of controlling elements for EW operations.

b. Signal. Reference the C-E annex to the order, the appropriate portions of the CEOI pertaining to EW operations. May provide an appendix including the restricted frequency list.

(Classification)

(Classification)

(Short title identification)

Acknowledgement instructions.

Last name of commander

Rank

AUTHENTICATION.

APPENDIXES: As needed. (May include division composite EW Target List and Restricted Frequency List.)

DISTRIBUTION:

(Classification)

APPENDIX F

Electronic Warfare Targeting Formats

Electronic warfare target lists, worksheets, and jamming schedules are critical tools in developing and cuing ESM and ECM missions. While certain ECM control measures give jamming system operators the latitude to engage targets freely, preplanned or on-call ECM missions usually have a greater effect in support of a specific operation. Preplanned ESM missions can provide key targeting data or combat information regarding enemy C^2 decisions.

Typical formats for preplanning EW missions are provided in this appendix, with brief descriptions of their use and the echelon at which they are provided.

BRIGADE ELECTRONIC WARFARE TARGET LIST WORKSHEET

Maneuver brigades develop this worksheet to identify their EW requirements. The brigade S3, S2, and the supporting IEW support element use the worksheet to prioritize EW targets that support the brigade's planned operation. This worksheet is forwarded to the division EW section in the DTOC for consolidation. The brigade Electronic Warfare Target List (EWTL) Worksheet includes identification of the unit to be targeted with its location, the type of communications activity to be jammed or reported, and information of reporting requirements. A format for this brigade worksheet is provided below.

BRIGADE EW TARGET LIST WORKSHEET

PRIORITY ESM	PRIORITY ECM	TIME WINDOW	TARGET UNIT	TARGET LOCATION	TARGET ACTIVITY	CONTROL MECHANISM	FEEDBACK/ COORDINATION

SAMPLE ENTRIES:

1	NA	310100Z-310400Z	fnd Tk Bn of 39 GMRD	NB448292	Report move from as area	NA	TACREP w/in 5 min
NA	1	310100Z-310130Z	RAG, 141 MRR	NB325310	Call for fire msns	Negative	EWMSNSUM

DIVISION COMPOSITE EW TARGET LIST

The EWS of the DTOC support element consolidates EW requirements from the brigade worksheets and adds division EW missions. The EWS uses the Division Composite EWTL to identify and prioritize all EW activities, and to identify whether division assets will execute the mission or if it will be requested of corps. The Division Composite EWTL is normally published as an appendix to the Division EW Annex. A format for the Division Composite EWTL is provided below.

DIVISION COMPOSITE EW TARGET LIST

PRIORITY ESM	PRIORITY ECM	TIME WINDOW	TARGET UNIT	TECH DATA?	TARGET LOCATION	TARGET ACTIVITY	EW UNIT	CONTROL MECHANISM	COORDI-NATION
SAMPLE ENTRIES:									
1	NA	310300Z-310400Z	HQ, 131 MRR	NO	UNK		Corps MI BN (AE)	NA	TACREP
NA	1	310001Z-310100Z	RECON 39 GMRO	YES	NBZZ7314	INTREPS	DIV MI BN	Negative	EWMSNSUM
NA	2	310100Z-310130Z	RAG, 141 MRR	YES	NB448292	Call for fire msns	DIV MI BN	On-off	EWMSNSUM

TCAE EW TARGET LIST/ JAMMING SCHEDULE

Based on the Division Composite EWTL and copies of the Brigade EWTL Worksheets, the MI battalion task organization and actual deployment, and the technical data available in the TCAE, a working board for EW missions will be maintained in the MI battalion TOC. Normally, one such board is maintained for each subordinate EW unit. The TCAE EWTL for each unit will include the status and capabilities of the systems in that platoon. This TCAE EWTL/Jamming Schedule (JS) will be used to list and monitor each EW mission and is the basis for asset tasking messages. It is updated constantly during the operation with input from the division EWS and the IEW support elements. While the EWTL at brigade and division are planning tools, the TCAE EWTL/JS is a management tool for the tasking of the C&J platoons, SIGINT processing platoon, and flight platoon. A format for this TCAE EWTL/JS is provided below.

TCAE EW TARGET LIST/JAMMING SCHEDULE WORKING BOARD

BOARD FOR _____ **PLATOON**

ASSETS:	STATUS:	LOCATION:	CAPABILITIES:	PERSONNEL:
_____	G A R	_____	_____	_____
_____	G A R	_____	_____	_____
_____	G A R	_____	_____	_____
_____	G A R	_____	_____	_____
_____	G A R	_____	_____	_____

PRIORITY ESM	PRIORITY ECM	TIME WINDOW	TARGET UNIT	TARGET LOCATION	TARGET ACTIVITY	TECH DATA FREQ	TECH DATA CSGN	CONTROL MECHANISM	COORDINATION	RESULTS

SAMPLE ENTRIES:

NA	1	310100Z-310200Z	RAG, 141 MRR	NB325310	Calls for fire msns	35.10 MHz	LION-34	On-off	EWMSNSUM to 2d Bde IEWSE	
1	NA	310300Z-310400Z	HQ, 131 MRR	Unknown	Location (LOB)	54.85 MHz	BEAR-62	NA	TACREP to TCAE	

APPENDIX G

Dissemination Devices

The following chart indicates some of the intelligence reports and summaries used at corps and below and the types of information or intelligence reported in each. This chart may be used to help determine which reports or summaries to select when reporting the types of information indicated in the left column of the chart.

Most of the formats and reporting criteria applicable to these reports/summaries are governed by International Standardization Agreements with the exception of SIGINT reports which are governed by US SIGINT Directives (USSID).

DISSEMINATION SUMMARIES AND REPORTS

ENEMY ACTIVITY	INTSUM	SITREP	PERINTREP	INTREP	IMAGERY REPORTS*	SIGINT TACREP
NBC	X	X	X	X	X	X
AIR	X	X	X	X	X	X
MOVEMENTS	X	X	X	X	X	X
NAVAL	X	X	X	X	X	X
LOGISTIC	X	X	X	X	X	X
AIRBORNE		X	X	X	X	X
IRREGULAR		X	X	X	X	X
EW		X	X	X	X	X
ENEMY OB						
MISSIONS				X		X
UNITS	X	X	X	X		X
PERSONALITIES	X			X		X
STRENGTH	X	X	X		X	X
UNIFORMS/INSIGNIA			X			
CAPABILITIES/VULNERABILITIES	X	X	X	X		X
NONEFFECTIVE UNITS		X	X			X
COMPOSITION & DISPOSITION			X	X	X	X
TACTICS			X			
TRAINING			X			
COMBAT EFFECTIVENESS		X	X			X
CODE NAMES/NUMBERS						X
RADIO FREQS/CALL SIGNS						X
COMM/NONCOM SECURITY			X			X
FWD TRACE	X	X				
POTENTIAL NUCLEAR TARGETS	X			X	X	X
OBSTACLES & BARRIERS	X	X	X		X	X
INSTALLATIONS, EVENTS, SIGHTINGS		X		X	X	X
ENEMY CAPTURED DOCU/EQUIP				X		
ESPIONAGE			X	X		
SABOTAGE			X	X		
WEATHER & TERRAIN	X		X			
FRIENDLY FWD TRACE		X				
LOCATION OF FRIENDLY UNITS		X				
RESULTS OF OPERATIONS		X				
PIR				X		

* • IN-FLIGHT REPORT
• RECONNAISSANCE EXPLOITATION REPORT
• INITIAL/SUPPLEMENTAL PROGRAMED INTERPRETATION REPORT
• RADAR EXPLOITATION REPORT

APPENDIX H

The Collection Plan

The collection plan has no prescribed format. The selection of a format at any particular headquarters is based on the requirements of that headquarters and the resources available for collection management. However, regardless of the format selected, it must follow the logical sequence of collection management described in Chapter 3. In addition, the plan must be easily adjustable to changing requirements, situations, and missions. This appendix provides two recommended formats which may be adjusted to fit specific requirements.

The intelligence collection plan worksheet is a valuable aid to collection management in planning and directing the collection effort. For many requirements, particularly those concerned with enemy capabilities and vulnerabilities, a written collection worksheet is advisable. The detail in which it is prepared, however, depends on the particular requirement to be satisfied and the extent to which the overall collection effort must be coordinated. At battalion and brigade, the collection plan worksheet is very informal. It may consist of a list of available collection means plus brief notes or reminders on current intelligence requirements and specific information that must be collected.

At corps and division, collection planning is more complex. The PIR of a corps commander often require painstaking analysis, and the coordination of the overall collection effort is a major undertaking. For that reason, written collection worksheets prepared at these echelons are very detailed. The following diagram shows a collection plan format suitable for division and corps. Brigades and battalions modify this format to fit their requirements.

COLLECTION WORKSHEET FORMAT

PRIORITY INTELLIGENCE REQUIREMENTS AND INFORMATION REQUIREMENTS	INDICATORS	SPECIFIC INFORMATION REQUIREMENTS	COLLECTION AGENCIES	PLACE AND TIME TO REPORT	REMARKS
	INSTRUCTIONS				
LIST PIR/IR. LEAVE SUFFICIENT SPACE TO LIST INDICATORS FOR EACH PIR/IR IN COLUMN 2.	LIST INDICATORS THAT WILL SATISFY EACH PIR.	LIST SPECIFIC INFORMATION REQUIRED TO SATISFY THE INDICATOR. KEY REQUIREMENTS TO NAI ON THE EVENT TEMPLATE IF POSSIBLE. THESE REQUIREMENTS FORM THE BASIS FOR SPECIFIC ORDERS AND REQUESTS.	PLACE AN X UNDER EACH AGENCY THAT CAN COLLECT THE REQUIRED INFORMATION. CIRCLE THE X WHEN AN AGENCY HAS BEEN SELECTED AND TASKED.	PLACE MAY BE A HEADQUARTERS OR UNIT. TIME MAY BE SPECIFIC, PERIODIC, OR AS OBTAINED.	INCLUDE MEANS OF REPORTING (VIA SPOT REPORT FORMAT); ESTABLISHED COMMUNICATIONS (MULTICHANNEL, FM, RATT), OR STATE "BY SOP" IF SOP CRITERIA APPLIES FOR RESPONDING TO COLLECTION REQUIREMENTS.
	EXAMPLE				
1. Will the enemy attack? If so, when, where, and in what strength? 2. ---	Massing of mech elements, artillery, and logistical support.	Enemy movement between ridge vic 5047-5042 to Seina Rivar. Rpt size and type unit, direction of movament, and termination pt. Special attention to NAI 3, 5, & 8.			

The following illustration provides an example of a completed collection worksheet using fictitious data.

CLASSIFICATION

UNIT: 52nd Inf Div (Mech)

COLLECTION PLAN

PERIOD COVERED: FROM H-12 Hours **TO** H+12 Hours

PRIORITY INTELLIGENCE REQUIREMENTS AND INFORMATION REQUIREMENTS	INDICATIONS (ANAYLSIS OF INTELLIGENCE REQUIREMENTS)
PIR 1. Will the enemy attack? If so, who, what, when, where, and in what strength?	a. Formation of RAGs & DAGs. b. Excessive barrage jamming. c. Massing of motorized rifle elements, tanks, artillery & logistic support. d. Movement of units forward.

AVENUE OF APPROACH — COORDINATES FM TQ 5720 TO UQ 9273

MOBILITY CORRIDOR NO — FM TO

NAMED AREA OF INTEREST	DISTANCE	TIME NET	TIME NLT	SPECIFIC ORDERS OR REQUESTS	OBSERVED TIME	I CORPS	II CORPS	23d ARMD	1st BDE	2d BDE	3d BDE	DIV ARTY	DISCOM	52d MI BN	52d MP CO	DIV ADA BN	DIV CAVSQDN	ENGR BN	G5	HOUR AND DESTINATION OF REPORTS	REMARKS
NAI 2	20km	H-12	1a H+4	Report formation of RAGs & DAGs for the following units: 67TD, 63TD, U/I MRD VIC UQ0617		x	x	⊗						⊗						As Obtained	As Needed
NAI 1	10km	H-12	1b H+12	Report jamming of all nets w/emphasis on CMD & control nets		x	x	x	⊗	⊗	⊗	⊗	⊗	x	x	x	x	x	x		
NAI 2	30km	H-12	1c H+12	Report number & type of vehicles in fwd assembly areas emphasis to vic TQ6020, TQ8218 UQ0617		⊗	x	x						⊗							
NAI 3	50km	H-12	1d H+1	Report of movement south out of fwd assembly areas vic highways 75, 23, 120, 36 & 7		⊗	x	x						⊗							

AVENUE OF APPROACH — COORDINATES FM TO

MOBILITY CORRIDOR NO — FM TQ 5901 TO TQ 8220

NAMED AREA OF INTEREST	DISTANCE	TIME NET	TIME NLT	SPECIFIC ORDERS OR REQUESTS	OBSERVED TIME
NAI					
NAI					
NAI					

AGENCIES TO BE EMPLOYED

I CORPS	II CORPS	23d ARMD	1st BDE	2d BDE	3d BDE	DIV ARTY	DISCOM	52d MI BN	52d MP CO	DIV ADA BN	DIV CAVSQDN	ENGR BN	G5

Briefly state specific information to be sought that will substantiate each indication.

Specific information needs become the basis for orders and requests to collect information

(List all available units that can be employed in the collection of required information)

Place an "X" under each unit that can acquire the specific information sought. Circle the "X" under the unit actually selected that will be assigned collection action

CLASSIFICATION

COLLECTION PLAN FORMAT

A visual file index, using 5x8 inch cards, is another method for maintaining a collection plan. In this method, a collection requirement is displayed across the bottom of a card. The remainder of the card may contain the following:

- ☐ Priority.
- ☐ Request or request number.
- ☐ Time requested and time when information will no longer be of value.
- ☐ Additional distribution of results.
- ☐ Collection agencies tasked and time.
- ☐ Time the answer was received.
- ☐ Answer.
- ☐ Time the answer was disseminated to the requestor.

The following illustrations provide examples of the visual file system.

COLLECTION COORDINATION VISUAL FILE FOLDER

PRIORITY: 1 REQUESTOR: G2, 52d DIV (M) TIME REQUESTED: 050200 MAY 82 ADDITIONAL DISTRIBUTION: NONE COLLECTION AGENCY TASKED: 5th CORPS REQUEST NO: RII 04 TIME REQUIRED: 052100 MAY 82 RESPONSE: TELS LOCATION VICINITY OF COORDINATES NB580160. TIME ANSWER DISSEMINATED: 052015 MAY 82	PRIORITY: REQUESTOR: TIME REQUESTED: ADDITIONAL DISTRIBUTION: COLLECTION AGENCY TASKED: REQUEST NO: TIME REQUIRED: RESPONSE: TIME ANSWER DISSEMINATED:
REQUEST LOCATIONS OF ANY TELS IN VICINITY OF COORDINATES NA430970, NB370180, AND NB580160.	
REQUEST LOCATIONS OF ANY METEOROLOGICAL ASSOCIATED RADARS IN VIC OF COORDS NA4397, NB3718, AND NB5816.	
REQUEST REPORT OF HEAVY VEHICLE MOVEMENT AND DIRECTION IN VICINITY OF COORDINATES NA660980 AND NB664014.	
REQUEST LOC OF ANY HEAVILY GUARDED AREA WHERE PERSONNEL HAVE BEEN EXCLUDED IN VIC COORDS NA430970, NB370180, AND NB580160.	
REQUEST LOCATIONS OF ANY 180MM GUN AND 240 MORTARS IN SECTOR.	

COLLECTION MANAGEMENT VISUAL FILE CARD

PRIORITY: 1
REQUESTOR: G2, 52d DIV (M)
TIME REQUESTED: 050200 MAY 82
ADDITIONAL DISTRIBUTION: NONE
COLLECTION AGENCY TASKED: 5th CORPS

REQUEST NO: RII 04
TIME REQUIRED: 052100 MAY 82

TIME: 052015 MAY 82

RESPONSE:
TWO TELS LOCATION VICINITY OF COORDINATES NB580160, UNDER CAM, LAUNCHERS ERECTED.

REQUEST LOCATIONS OF ANY TELS IN VICINITY OF COORDINATES NA430970, NB370180, AND NB580160.

Priorities can be shown by using different colored cards or index tabs. For example, if a request must be answered within a certain timeframe, a red card or index tab will highlight its importance to the collection manager, no matter how many shift changes take place.

The cards can be grouped in the visual files in a number of ways: OB factors, NAIs, requestor, or collector. In each operation the file may start out one way and, by necessity, be changed as the situation changes. This can be accomplished quickly as the cards are easily manipulated.

When the collection requirement is satisfied, the card is removed from the visual files. The remainder of the cards are not disrupted. The 5x8 card can then be placed in a small file organized by geographic areas. This enables the collection manager to build a data base on the responsiveness of the collection agencies within the geographical areas.

If the visual file method is used, the collection manager must maintain two charts. One chart is used to depict the PIR and IR which drive the collection effort. The second chart lists the available units and agencies, and those tasked with each requirement. This chart is needed to prevent overloading or overlooking any single available collector. Both charts are shown in the following illustrations.

COMMANDER'S PIR/IR	
PIR	IR
1. Does the enemy intend to deploy nuclear weapons in the the division sector?	1. What is the location of the second echelon? When will it be committed? 2. What avenue of approach will the enemy use into FULDA?

AVAILABLE AGENCIES AND TASKING	
AGENCIES	TASKING
MI BN	RII-01
DIVARTY	RII-03
ENGR BN	
ARMORED CAVALRY SQD	
BRIGADES	
CORPS	RII-02, RII-04, RII-05
ADJACENT DIVISIONS	

APPENDIX I

Tactical Special Security Operations

INTRODUCTION

The SSO system is a DOD security and communications system used to transmit SCI between commands and services and to and from national-level intelligence agencies using the Defense Special Security Communications System (DSSCS), the Armed Forces Courier Service (ARFCOS), or secure facsimile systems. It also secures SCI and provides for its widest possible dissemination consistent with applicable security guidelines. In addition, the system provides privacy communications (EYES ONLY) service to general officers, promotable colonels, and designated equivalent-grade civilians.

The ACSI-DA is responsible for operation of the DA portion of the SSO system. This is accomplished through the US Army Special Security Group (USASSG). USASSG is responsible for direction and coordination of all Army SCI operations and facilities. It directly commands and controls all nontactical EAC SSOs and exercises security jurisdiction over tactical SSO operations at corps and below. This security jurisdiction includes advice and assistance relating to the security, handling, and use of SCI, billet management, completeness of documents requesting SCI products, and inspections of SCI facilities and SSO operations. It also includes training for tactical SSOs, both active and reserve.

In the training environment the SSO has the added responsiblity of controlling the distribution of both "real world" and exercise SCI traffic. Although exercise traffic in most instances is written for a particular training exercise, the SSO must bear in mind that exercise data pertaining to operational forces' OB, organization, operational indicators, formations, and use of terrain can readily become "real world" traffic in wartime. It is imperative that the tactical SSO realize that special security functions in the field environment are the same in peacetime as in war. Additionally, the SSO in the field will have to comply with the tactical commander's OPSEC policy.

SECURITY STANDARDS FOR FIELD OPERATIONS

Minimum physical security requirements for field sensitive compartmented information facilities (SCIFs) are specified in Chapter 7, Defense Intelligence Agency Manual 50-3. SSOs must review and update their unit field SOP to ensure that security standards are applied. The requirements identified in the following paragraphs should be improved upon as the enemy situation, terrain, and time dictate.

When the SCIF area is located within the confines of the supported command's TOC and defensive perimeter, the SCIF area must be conspicuously marked by a physical barrier. When the SCIF area is outside the supported headquarters TOC and defensive perimeter, the SCIF area should be fenced with triple-strand concertina wire. However, if the SCIF is subject to frequent moves (once per 8- to 10-hour span), single-strand concertina or a similar type of wire may be employed.

The SCIF perimeter must be guarded by fixed or patrolling armed guards. The types of weapons and ammunition issued to the guards will be prescribed by the supported command. The use of deadly force should be addressed in the unit tactical SOP.

Access to the SCIF area is restricted to a single gate or entrance. The gate or entrance to the SCIF area must be guarded on a 24-hour basis. A landline between the entrance point guard and the SSO administrative area will facilitate the rapid and efficient entry of cleared personnel.

The SSO maintains a current access roster that includes SCI-indoctrinated personnel of the local command, very important

persons, observers, umpires, controllers, augmentees, and other authorized personnel requiring access. Access will be restricted to those on the access roster. Access by others (such as maintenance personnel) may become necessary, but must be minimized and controlled by the SSO.

A minimum of two SCI-indoctrinated personnel will be present in the SCIF(s) at all times.

Communications, both wire and radio if possible, will be established and maintained with the security guards. Use of field phones is authorized if a filter or some other suitable means is used to preclude inadvertent disclosure of information over open lines or circuits. One acceptable method would be to utilize a TA 312 connected to a switchboard in the SCIF. The internal phone lines are connected to the switchboard only when talking. At all other times the internal phone lines will be disconnected. Use of FM radios in SCIFs is a potential security hazard, but, if used, radios should be as far away as possible from classified discussion areas and other communications equipment. When FM radios are transmitting, classified discussion must be kept to an absolute minimum consistent with operational necessity.

Emergency destruction and evacuation plans will be current and maintained in the facility.

When not in use, and during SCIF relocation, SCI material will be locked in GSA-approved containers. If for some reason the above minimum standards cannot be met, SSOs should request a waiver in accordance with procedures outlined in Chapter 7 of the SSO Handbook.

COORDINATION REQUIREMENTS

The following guidelines apply to the planning and preparation for field operations. Although the responsibility for SSO operations rests with the G2, in most cases the SSO effects coordination in the name of the G2.

COMMUNICATIONS

The SSO coordinates with the local unit headquarters commandant and, as necessary, with the signal battalion for teletype circuits, landlines, establishment and restoration priority, key lists, backup systems (usually courier), maintenance of on-site communications equipment, and any unique communications procedures such as changing the teletype word-per-minute rate to achieve system compatibility with other SSOs. The SSO will not be the only element in the CP with SCI communications. MI units have access to a variety of SCI-secure communications facilities. Requirements to support several locations can be met by combining equipment to meet both requirements or in agreements to serve as alternative deliverers.

TRANSPORTATION

Vehicles for the SSO should be requested through headquarters and headquarters company, corps, or division. Should additional vehicles be necessary to support several dispersed field SCIFs, they should be requested through the headquarters and headquarters company commander.

MILITARY POLICE

The SSO coordinates with the headquarters commandant or the MP unit supporting the command for SCIF-entrance point and roving guards and the reaction force. The SSO should provide SCIF guards an SOP that addresses, but is not limited to, control of the SCIF, criteria for admittance, actions during attack, use of deadly force, and inspection of notebooks and briefcases. Alternate SSOs supporting separate brigades or TCAEs may have to employ non-MP guards. Guards themselves need not be SCI indoctrinated provided they conduct roving patrols and control accesses outside the protective perimeter.

EXERCISE COMMUNICATIONS INTELLIGENCE

Chapter 7, DOD Directive 5200.17(M2), permits the use of exercise COMINT during exercises provided that the material is handled in accordance with existing regulations governing the security, use, and dissemination of real-world COMINT material.

The authority to approve the use of exercise COMINT is governed by Chapter 5, AR 380-35. The chief, TCAE should be consulted regarding current guidelines contained in the appropriate USSID. When used, exercise COMINT must be physically separated and handled separately from real-world COMINT. In some commands, the SSO performs the sanitization, while in others the ASPS sanitizes under the supervision of the SSO. Whatever the process, the SSO is ultimately responsible for ensuring sanitization and must ensure that all evidence of COMINT is removed from documents disseminated outside the SCIF. When exercise COMINT is used, a report is required by paragraph 5-4c, AR 380-35. The proper authority for use of exercise COMINT is given to the MACOM commander in CONUS and outside continental United States (OCONUS) or is delegated from the unified command OCONUS. The proper authority must designate in writing those staff sections that can act in the commander's behalf. Noncodeword COMINT-based reporting under the provisions of USSID 369 and USSID 316 is exempt.

BLACK BOOK

The SSO coordinates with the G2, command group, and other authorized recipients, to determine delivery requirements. General officers probably will have limited time for the black book during an exercise or contingency situation. Due to security constraints, it is recommended that the G2 and SSO restrict delivery to the general officer level but have the black book available in the SCIF for other indoctrinated personnel with a need to know.

EYES ONLY MESSAGES

The SSO coordinates with the G2 and command group. Due to the importance of EYES ONLY messages to the command, the SSO must know how and when to reach authorized users and be aware of unusual transmission procedures. The SSO must plan to provide service during periods when SSO communications systems are not operational or not yet in place. Situations where this contingency should be considered include the aerial port of debarkation/seaport of debarkation (APOD/SPOD), the prepositioning of materiel configured to unit sets (POMCUS) draw, and movement to various marshalling and assembly areas. Eligible users should be reminded of the parallel "Personal For" channel provided by the signal corps.

VISIT CERTIFICATION

The SSO coordinates visits with the SSOs of higher, lower, and adjacent participating units, and with the secretary of the general staff's protocol and joint visitors bureau, if established. Visit certification messages should be received by the SSO in advance of the planned visit. Visit certifications should reflect personnel traveling with the visiting VIP who are authorized to receive EYES ONLY messages.

PERSONNEL AUGMENTATION

The SSO coordinates with the G2 for personnel augmentation. Additional personnel may be needed to operate a garrison SCIF and one or more field SCIFs simultaneously. SSO augmentation personnel should be given sufficient time prior to movement to become familiar with SSO equipment and procedures.

OPERATIONS SECURITY

OPSEC includes all actions taken to prevent the enemy from gaining knowledge of operations. Sound physical security and communications security procedures must be followed for a successful OPSEC program. The SSO coordinates with the command's CI analysis section for information on the multidisciplined hostile threat. The SSO should consider the following security measures:

- ☐ Separating trash and paper (including all forms of written material and carbons).
- ☐ Destruction means.
- ☐ Screening of all outgoing material.
- ☐ Appointing and briefing additional SCI couriers.
- ☐ Briefing all SCIF personnel on SCI handling and security.

- ☐ Obtaining TOC passes.
- ☐ Using wire instead of radio.
- ☐ Using authorized authentication procedures and codes.

SUPPLIES AND SERVICES

The SSO coordinates requirements for protective wire and camouflage nets with the corps or division headquarters and headquarters company.

SPECIAL SECURITY OFFICERS COORDINATION

Coordination between SSOs participating in a joint training exercise is necessary to ensure that information impacting on SSO operations is disseminated in a timely manner.

FIELD SCIF CONFIGURATION AND ESTABLISHMENT

Due to the importance of IEW to tactical units, SSOs are responsible for the technical security supervision of increasing numbers of SCIFs during exercises. In addition to supporting TOCs with SCIFs, MI operations centers will also serve as SCIFs, stretching SSO supervision to the maximum. As described earlier, the SSO has overall responsibility for all SCI activities. To facilitate supervision of multiple locations, an assistant SSO may be appointed on orders. The actual establishment of a field SCIF will depend on a number of factors, including doctrinal requirements and the real-world considerations of fighting a well-armed, increasingly technologically oriented enemy versus participation in a controlled exercise. The SSO, G2, G3, and MI unit commander should consider the following when planning for the establishment of a SCIF:

- ☐ SOP of local command and supported unit.
- ☐ Terrain.
- ☐ Enemy capabilities.
- ☐ Rear area threat.

A SCIF must have its own separate perimeter no matter where it is located. SCIF perimeters should have restricted area signs displayed around them and, due to SCI holdings, should be designated nonplay areas during exercises. In exercise situations, the SCIFs should be placed off limits in the exercise directive and the G2 and chief umpire or controller should publicize that fact.

In most units the location of the SCIF will be directed by the G2 in coordination with the G3. The priorities assigned to the work needed to establish a SCIF, once the SSO arrives on site, vary according to command SOP and current conditions. However, the work will include the following tasks:

- ☐ Position vehicles.
- ☐ Ready work areas for use.
- ☐ Establish communications.
- ☐ Establish SCIF perimeter.
- ☐ Camouflage the area.
- ☐ Control access using guards or SSO personnel.
- ☐ Declare area secure.
- ☐ Begin SCI operations.

Special attention must be paid to coordination of SSO requirements with the division or corps headquarters commandant. This officer is responsible for the physical plant of the division or corps TOC. He operates in the name of the division or corps chief of staff and has the authority to overrule the SSO regarding SCIF siting. The SSO must carefully orient the headquarters commandant regarding tactical SCIF requirements. The SSO must be aware of TOC relocation plans and schedules. The SSO must also be aware when the TOC perimeter has been dropped since a reduction in overall security has a negative impact on SCIF protection.

MI UNIT RESPONSIBILITIES

The MI unit has responsibility for SCI operations associated with MI unit operations. In supporting its operations, the MI unit may find it necessary to hold data base material and otherwise process SCI at the TCAE and at other locations. In any case,

these locations must meet field SCIF standards as discussed in this appendix and in relevant portions of Defense Intelligence Agency Manual 50-3. A responsible officer must be assigned on orders as an alternate SSO exercising SCI security responsibilities under the jurisdiction of the division SSO. These alternate SSOs can perform other tasks such as MI unit billet management, indoctrinations, debriefing, sanitization, and decompartmentation. It must be remembered, however, that all SSO operations in the division are the staff responsibility of the G2 and are supervised by the division SSO. Thus, close coordination between the SSO and MI unit alternate SSOs is essential. Personnel assigned as alternate SSOs must receive the same SSO training as the division SSO.

The functions and responsibilities in the preceding descriptions of SSO operations were oriented toward the division. They are also applicable to the corps SSO and MI brigade. In addition, the corps SSO will have the responsibility of ensuring security for assigned AN/TSQ-134(V), Interim Tactical ELINT Processor, Digital Imagery Test Bed, the tactical user terminal, and any other SCI-processing systems. When not located in a CTOC SCIF area, these systems must be supervised by an alternate SSO acting for the corps SSO.

Further information concerning the SSO system and SCI security responsibilities may be found in AR 380-28, AR 380-35, TB 380-35, DIAM 50-3, and the unofficial SSO Handbook, published by the USASSG.

GLOSSARY

AAA	antiaircraft artillery
AAFES	Army and Air Force Exchange Service
AASLT	air assault
abn	airborne
AC	active component
ACC	area coordination centers
ACofS	Army Chief of Staff
ACR	armored cavalry regiment
ACSI	Assistant Chief of Staff for Intelligence
AD	air defense
ADA	air defense artillery
ADC	area damage control
ADC-M	assistant division commander-maneuver
ADP	automatic data processing
ADPS	automatic data processing system
AE	aerial exploitation
AIDES	Analyst's Intelligence Display and Exploitation System
AIRES	Advanced Imagery Requirements and Exploitation System
ALO	air liaison officer
AM	amplitude modulated
AMC	US Army Materiel Command
ammo	ammunition
AO	area of operations
AOE	Army of Excellence
APOD	aerial port of debarkation
appl	application
AR	Army regulation
ARFCOS	Armed Forces Courier Service
arty	artillery
ASA	Automated Systems Activity
ASAS	All-Source Analysis System
ASG	area support group
ASL	authorized stockage list
ASOC	air support operations center
ASP	ammunition supply point
ASPS	all-source production section
assy	assembly
ATP	ammunition transfer point
AVIM	aviation intermediate maintenance
avn	aviation
AVUM	aviation unit maintenance
AWS	Air Weather Service
BAT-D	battlefield deception
BCE	battlefield coordination element
bde	brigade
BCOC	base cluster operations center
BDLT	base defense liaison team
BDOC	base defense operations center
BICC	battlefield information coordination center

bn	battalion
BOMREP	bombing report
btry	battery
C^2	command and control
C^3	command, control, and communications
C^3CM	command, control, communications countermeasures
C^3I	command, control, communications, and intelligence
CA	civil affairs
C&J	collection and jamming
CAS	close air support
cbt	combat
CCEWS	Combined Commander's Electronic Warfare Staff
C-E	Communications-Electronics
CEOI	Communications-Electronics Operation Instructions
CEWI	combat electronic warfare and intelligence
CFA	covering force area
chem	chemical
CI	counterintelligence
CIA	Central Intelligence Agency
CIC	combined intelligence center
CLSU	COMSEC logistic support unit
CM&D	collection management and dissemination
CMO	civil/military operations
CMT	crisis management team
co	company
COINS	Community On-Line Intelligence System
coll	collection
COMCAT	Character Oriented Message Catalog
COMINT	communications intelligence
comm	communications
comp	component
COMSEC	communications security
CONUS	continental United States
coords	coordinates
COP	command observation post
COSCOM	corps support command
CP	command post
CSA	corps support activity
CSG	corps support group
CSS	combat service support
CTOC	corps tactical operations center
ctr	center
CUBIC	Common Users Baseline for the Intelligence Community
DA	Department of Army
DCS	Defense Communications System
DCSOPS	Deputy Chief of Staff for Operations and Plans
decon	decontamination
DF	direction finding
DIA	Defense Intelligence Agency
DIAOLS	Defense Intelligence Agency On-Line System

DIE	Defense Intelligence Estimate
DISCOM	division support command
disem	dissemination
div	division
divarty	division artillery
DLIC	detachment to be left in contact
DMA	Defense Mapping Agency
DMSO	division medical supply officer
DOD	Department of Defense
DP	decision points
DS	direct support
DSO	defense source operations
DSSCS	Defense Special Security Communications System
DST	decision support template
DTG	date-time group
DTOC	division tactical operations center
DZ	drop zone
EAC	echelons above corps
EACIC	EAC intelligence center
ECB	echelons corps and below
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
EEFI	essential elements of friendly information
ELINT	electronic intelligence
elm	element
EMCON	emission control
EMP	electromagnetic pulse
engr	engineer
EOB	electronic order of battle
EOD	explosive ordnance disposal
EPW	enemy prisoner of war
ESM	electronic warfare support measures
EW	electronic warfare
EWS	electronic warfare section
EWTL/JS	electronic warfare target list/jamming schedule
EXJAM	expendable jammers
FA	field artillery
FAIO	field artillery intelligence officer
FARP	forward arming and refueling points
FDC	fire direction center
FEBA	forward edge of the battle area
FISINT	foreign instrumentation signals intelligence
FIST	fire support team
FLOT	forward line of own troops
flt	flight
FM	field manual/frequency modulated
FRAGO	fragmentary orders
FSE	fire support element
FSO	fire support officer
FSTC	Foreign Science and Technology Center

FTI	fixed target indicators
fwd	forward
G1	Assistant Chief of Staff, G1 (Personnel)
G2	Assistant Chief of Staff, G2 (Intelligence)
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, G4 (Logistics)
G5	Assistant Chief of Staff, G5 (Civil Affairs)
GS	general support
GSA	General Services Administration
GRU	General Staff's Main Intelligence Directorate (USSR)
GSR	ground surveillance radar
HF	high frequency
HHC	headquarters and headquarters company
HHOC	headquarters, headquarters and operations company
HHSC	headquarters, headquarters and service company
HPT	high payoff target
HQ	headquarters
HHT	headquarters headquarters troop
HNS	host-nation support
HUMINT	human intelligence
HVT	high value target
hvy	heavy
IA	imagery analysis
I&W	indications and warning
ICD	imitative communications deception
IDHS	Intelligence Data Handling Systems
IDP	initial delay position
IED	imitative electronic deception
IEW	intelligence and electronic warfare
IEWSE	intelligence and electronic warfare support element
IMINT	imagery intelligence
INCD	imitative noncommunications deception
info	information
INSCOM	Intelligence and Security Command
intcp	intercept
intel	intelligence
intg	interrogate/interrogation
INTREP	intelligence report
INTSUM	intelligence summary
IPAC	Intelligence Center Pacific
IPB	intelligence preparation of the battlefield
IR	information requirements
IRDL	Imagery Reconnaissance Directives List
ISE	intelligence support element
ITAC	Intelligence and Threat Analysis Center

J2	Intelligence Directorate
J3	Operations Directorate
J6	Communications-Electronics Directorate
JCEWS	joint commander's EW staff
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Center
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JOC	joint operations center
JSEAD	joint suppression of enemy air defenses
J-TENS	Joint-Tactical Exploitation of National Systems
JTF	joint task force
KGB	Committee for State Security (USSR)
km	kilometer
LIC	low intensity conflict
LLVI	low-level voice intercept
LOB	line of bearing
LOC	lines of communication
loc	location
LOS	line of sight
LRSD	long range surveillance detachment
lt	light
LZ	landing zone
MAAG	Military Assistance Advisory Group
MACOM	major Army command
maint	maintenance
MAXI	Modular Architecture for the Exchange of Intelligence
MBA	main battle area
MC	mobility corridors
MCD	manipulative communications deception
MCS	master control station
mech	mechanical
MED	manipulative electronic deception
MEDSOM	medical, supply, optical, maintenance
METT-T	mission, enemy, terrain, troops, and time available
MI	military intelligence
MIJI	meaconing, intrusion, jamming, and interference
MMC	Materiel Management Center
MNCD	manipulative noncommunications deception
MOPP	mission oriented protective posture
MORTREP	Mortar Bombing Report
MP	military police
MRR	motorized rifle regiment
MR/TK	motorized rifle/tank
MST	maintenance support team
MTI	moving target indicator
MTM	mission tasking message

NAI	named area of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, chemical
NCA	national command authority
NETCAP	national exploitation of tactical capabilities
NIE	National Intelligence Estimate
NIS	national intelligence survey
NONCOM	noncommunications
NPCC	National Planning Coordination Center
NPIC	National Photo Interpretation Center
NSA	National Security Agency
OB	order of battle
OCOKA	***o***bservation and fields of fire ***c***oncealment and cover ***o***bstacles ***k***ey terrain ***a***venues of approach and mobility corridors
OCONUS	outside continental United States
OMG	operational maneuver group
OP	observation post
op	operations
OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
PACOM	Pacific Command
PCAC	primary control and analysis center
PDSC	Pacific Command Data System Center
PERINTREP	periodic intelligence report
PERINTSUM	periodic intelligence summary
PIR	priority intelligence requirements
PL	phase line
PLL	prescribed load list
plt	platoon
POL	petroleum, oils, and lubricants
POMCUS	prepositioning of overseas materiel configured to unit sets
prep	preparation
proc	processing
PSYOP	psychological operations
pt	point
QSTAG	Quadripartite Standardization Agreement
RADIAC	radiation, detection, indication, and computation
RAOC	rear area operations center
RATT	radio teletypewriter
RC	reserve component
REC	radio electronic combat (not a US term)

regt	regiment
reinf	reinforced
REMBASS	Remotely Monitored Battlefield Sensor System
REMS	remotely employed sensors
RF	radio frequency
RII	request for intelligence information
ROK	Republic of Korea
ROO	rear operations officer
rpt	report
RSTA	reconnaissance, surveillance, and target acquisition
RTOC	regimental tactical operations center
S1	Adjutant (US Army)
S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
S4	Supply Officer (US Army)
S5	Civil Affairs (US Army)
S&T intelligence	scientific and technical intelligence
SALUTE	size, activity, location, unit, time, and equipment
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SDP	second delay position
SDIE	Special Defense Intelligence Estimate
sec	section
SED	simulative electronic deception
SHELREP	shelling report
sig	signals
SIGINT	signals intelligence
SIGSEC	signal security
SIR	specific information requirements
SITMAP	situation map
SLAR	side-looking airborne radar
SOLIS	SIGINT On-Line Intelligence System
SOP	standing operating procedure
SOTI	security, operations, training and intelligence
SPO	security, plans, and operations
SPOD	seaport of debarkation
spt	support
sqd	squad
SSA	supply support activity
SSM	surface-to-surface missile
SSO	special security officer
sta	station
STANAG	Standardization Agreement
STOL	short takeoff and landing
SUPINTREP	supplementary intelligence report
survl	surveillance
svc	service
SWO	staff weather officer
TA	target acquisition/theater Army
TAACOM	Theater Army Area Command

tac	tactical
TACC	tactical air control center
TACFIRE	tactical fire direction computer system
TACP	tactical air control party
TACREP	tactical reports
TAI	target area of interest
T&A	transcription and analysis
TB	technical bulletin
TCAE	technical control and analysis element
TC&D	tactical cover and deception
TCF	tactical combat force
TE	tactical exploitation
TEL	transporter-erector-launcher
TENCAP	tactical exploitation of national capabilities
tm	team
TM	training manual
TMDE	test, measuring, and diagnostic equipment
TOC	tactical operations center
TOE	Tables of Organization and Equipment
TPL	timed phase line
TRADOC	United States Army Training and Doctrine Command
TREE	transient radiation effects on electronics
TS	top secret
TST	time-sensitive target
TVA	target value analysis
UHF	ultra high frequency
USAF	United States Air Force
USAICS	United States Army Intelligence Center and School
USAINSBD	United States Army Intelligence and Security Board
USAREUR	United States Army, Europe
USASSG	United States Army Special Security Group
USIA	United States Information Agency
USSID	United States Signals Intelligence Directive
UW	unconventional warfare
VHF	very high frequency
vic	vicinity
VTOL	vertical takeoff and landing
WETM	weather team
xmsn	transmission
xplt	exploitation

REFERENCES

REQUIRED PUBLICATIONS

Required publications are sources which users must read in order to understand or to comply with this publication.

Field Manuals (FMs)

100-5	Operations

RELATED PUBLICATIONS

Related publications are sources of additional information. They are not required in order to understand this publication.

Army Regulations (ARs)

37-55	Uniform Depot Maintenance Cost Accounting and Production Reporting System
380-Series	Security
380-28 (O)	The Army Special Security Officer and Office System
380-35 (S)	Department of the Army Communications Intelligence Security Regulations (U)
381-Series	Military Intelligence
525-22 (S)	Electronic Warfare (EW) Policy (U)
530-Series	Operations and Signal Security
710-2	Supply Policy Below the Wholesale Level
750-1	Army Materiel Maintenance Concepts and Policies

Field Manuals (FMs)

1-100	Combat Aviation Operations
1-500	Army Aviation Maintenance
3-4	NBC Protection
3-5	NBC Decontamination
3-100	NBC Operations
5-30	Engineer Intelligence
5-146	Engineer Topographic Units
6-121	Field Artillery Target Acquisition
17-95	Cavalry Operations
19-1	Military Police Support for AirLand Battle
21-31	Topographic Symbols
21-32	Topographic Support
24-1	Combat Communications
24-33	Communications Techniques: Electronic Counter-Countermeasures
31-11	Doctrine For Amphibious Operations
31-12	Army Forces in Amphibious Operations (The Army Landing Forces)
31-70	Basic Cold Weather Manual
31-71	Northern Operations

32-16 (C)	ECM Handbook (U)
33-1	Psychological Operations
34-Series	Intelligence and Electronic Warfare
34-2 (S)	Collection Management (U)
34-3	Intelligence Analysis
34-10	Division Intelligence and Electronic Warfare Operations
34-25	Corps Intelligence and Electronic Warfare Operations
34-35	Armored Cavalry Regiment Intelligence and Electronic Warfare Operations
34-37	Echelons Above Corps Intelligence and Electronic Warfare Operations
34-40 (S)	Electronic Warfare Operations (U)
34-52	Intelligence Interrogation
34-60	Counterintelligence
34-60A (S)	Counterintelligence Operations (U)
34-62	Counter-Signals Intelligence (C-SIGINT) Handbook
34-80	Brigade and Battalion Intelligence and Electronic Warfare Operations
34-81	Weather Support for Army Tactical Operations
44-1	Air Defense Artillery Reference Handbook
55-40	Army Combat Service Support Air Transport Operations
71-101 (HTF)	Infantry, Airborne, and Air Assault Division Operations (How to Fight)
90-2	Battlefield Deception
90-3 (HTF)	Desert Operations (How to Fight)
90-6	Mountain Operations
90-10 (HTF)	Military Operations on Urbanized Terrain (MOUT) (How to Fight)
90-13 (HTF)	River Crossing Operations (How to Fight)
90-14	Rear Battle
100-2-1	Soviet Army Operations and Tactics
100-2-2	Soviet Army Specialized Warfare and Rear Area Support
100-2-3	The Soviet Army Troops Organization and Equipment
100-10	Combat Service Support (How to Support)
100-20	Low Intensity Conflict
100-27	US Army/US Air Force Doctrine For Joint Airborne Tactical Airlift Operations
101-5	Staff Organization and Operations
101-5-1	Operational Terms and Symbols

Technical Bulletin (TB)

380-35 (C)	Security, Use, and Dissemination of Sensitive Compartmented Information (SCI) (U)

Miscellaneous Publications

DIAM 50-3 (C)	Physical Security Standards for Sensitive Compartmented Information Facilities (U)
DOD 5200.17(M2) (TS)	Special Security Manual (U)
JCS Pub 1	Dictionary of Military and Associated Terms
JCS Pub 12 (S)	Tactical Command and Control Procedures for Joint Operations (U)

DA Pam 550-Series	Area Handbooks
DA Pam 710-2-1	Using Unit Supply System Manual Procedures
DA Pam 710-2-2	The Supply Support Activity (SSA) Supply System
USSID 316 (S-CCO)	Non-Codeword Reporting Criteria (U)
USSID 369 (SCW)	Tactical Reporting (U)

COMMAND PUBLICATIONS

Command publications cannot be obtained through Armywide resupply channels. Determine availability by contacting the address shown. Field circulars expire three years from the date of publication unless sooner rescinded.

Field Circulars (FCs)

6-20-10	Fire Support Targeting, USA Field Artillery School, Ft Sill, OK, May 85
34-118/6-34-10	The Targeting Process, USA Field Artillery School, Ft Sill, OK and USA Intelligence Center and School, Ft Huachuca, AZ, May 85

INDEX

air defense artillery 2-20
air-land battle 1-1, 2-4
area of interest 1-3
area of operations 1-2
automated intelligence support 3-62, 3-65
  all-source analysis system 3-66
aviation 2-21

battlefield information coordination center 2-3, 2-4, 2-24

collection management 3-3, 3-21, 11-15
collection plan 3-21, 3-36, 3-59, H-1
collection resources 2-16
combat information 2-13, 2-20, 3-24, 3-61
command, control, and communications countermeasures 1-3
  CI 2-41, 4-15
  EW 2-41, 5-0, 5-7
command relationships 6-0
communications 5-12, 6-4
counterintelligence 1-4, 2-19, 4-1, 4-10

data base 3-10, 3-38
deception 2-19, 4-1, 4-13
  battlefield deception cell 2-31, 2-41
  CI support 2-19, 4-13
  electronic 5-5

electronic warfare 1-3, 2-16, 5-1
  control mechanisms 5-12
  ECCM 1-3, 2-18,
  ECM 1-3, 2-18, 5-2
  ESM 1-3, 2-18, 2-34
  planning 5-10
  principles 5-9
  targeting 5-7, F-0
engineers 2-21

field artillery 2-7, 2-20

G2 2-3, 2-5, 2-30, 3-3, 4-6
G3 2-3, 2-5, 2-30, 3-3, 4-6
ground surveillance radar 2-14, 2-28

intelligence and electronic warfare
  mission 1-1
  system 2-1, 2-20
intelligence, categories of targets 2-14
intelligence cycle 2-8
intelligence preparation of the battlefield 1-1, 3-1, 3-3, 11-14
  battlefield area evaluation 3-5, A-1
  decision points 3-20
  named areas of interest 3-15
  rear area 3-15, 11-14
  target areas of interest 3-19
  templates 3-4
    decision support 3-19
    doctrinal 3-12
    event 3-15
    situation 3-15
  terrain analysis 3-7, 3-10
  threat evaluation 3-10
  threat integration 3-10
  weather analysis 3-9
intelligence resources 3-26
  armored cavalry regiment 2-38, 2-48
  battalion 2-24, 2-48
  brigades 2-26, 2-48
  company 2-22
  corps 2-41, 2-48
  departmental 2-47
  division 2-30, 2-48
  echelons above corps 2-45, 2-48
  rear area 11-16
  separate brigade 2-38, 2-48
intelligence, types of 2-7
  human 2-13
  imagery 2-14
  operational 2-10
  scientific & technical 2-14, 3-57, 3-65
  signal 2-13, 2-34
  strategic 2-9
  tactical 2-11

long range surveillance detachment 2-34
low intensity conflict 12-5

maintenance 14-7
military intelligence battalions
  aerial exploitation 2-43
  CEWI 2-34
  operations 2-42

tactical exploitation 2-42
tactical exploitation (reserve component) 2-43
military intelligence brigade (CEWI) 2-36, 2-41, 11-14
military intelligence companies
armored cavalry regiment 2-38
collection and jamming company, heavy division 2-28, 2-32, 2-34
collection and jamming company, light division 2-28
company teams 2-26, 6-1
electronic warfare company 2-34
intelligence and surveillance company 2-34
separate brigade 2-38

OPSEC 11-15, I-3
CI support 2-19, 4-1, 4-6

psychological operations 2-21

QUICKFIX flight platoon 2-36, 2-39

rear area operations 4-10, 11-1
center 11-6, 11-8
CI support 2-19, 4-10
IPB 11-14
reports G-1
electronic warfare annex 5-14, E-1
electronic warfare estimate 5-14, D-1
imagery 3-64
intelligence annex 3-62, C-1
intelligence estimate B-1
INTREP 3-63
INTSUM 3-62, 3-63
interrogation 3-64
PERINTREP 3-62, 3-63, 3-64
PERINTSUM 3-64
S&T intelligence 3-65
spot 3-62
SUPINTREP 3-63
weather forecasts 3-64

signal security 2-19
situation development 1-1, 3-1, 11-15
special security officer 2-3, I-1
standard tactical missions 6-0
supply 14-1

tactical operations center support element 2-3, 2-30, 2-32, 2-41
ASPS 2-32, 3-10, 3-20, 3-22, 3-59
CM&D 2-32, 3-20
CI analysis 2-33, 2-34
EWS 2-31, 2-33, 5-1
FAIO 2-31, 2-33, 3-60
OPSEC staff element 2-31, 2-33, 2-34
terrain team 2-33
weather team 2-33
target development 1-1, 3-1, 3-51, 8-2, 11-15
tasking flow 3-33
task organization 6-1
technical control and analysis element 2-33

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

R. L. DILWORTH
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army, USAR, and ARNG: To be distributed in accordance with DA Form 12-11A, Requirements for Intelligence and Electronic Warfare Operations (Qty rqr block no. 1117).

☆ U.S. G.P.O. 1987-726-041:41113

3000020914

PIN: 056073-000